



UNCLASSIFIED

Net-Ready Key Performance Parameter

LTC Tom Gaetjen

J6

Agenda



- **Set Stage**
- **IER Approach**
- **Net Ready Approach**
- **Net Ready Key Performance Parameter (NR KPP)**
 - **Net-Centric Operations and Warfare (NCOW) Reference Model**
 - **Integrated Architectures**
 - **Key Interface Profiles**
 - **Information Assurance**
- **Program migration to the NR KPP (examples)**
- **NR KPP status**
- **Complimentary and Corresponding Systems**

Revised DODD 5000.1, DODI 5000.2 and DOD 5000.2R - USD-AT&L

DODD 4630.5 & DODI 4630.8 - OASD-NII

Capabilities

CJCSI 3170 (J8)

- Capability Validation Process/Procedures
- ICD, CDD, CPD Format
- NET READY KPP

CJCSI 6212 (J6)

- Interoperability and Supportability Certification and Testing
- Methodology for Net Ready KPP Development /Validation

Acquisition

Information Support Plan (OASD-NII)

Operational/System s/Technical Architecture Infrastructure Support

Testing

TEMP

Systems specs accurately reflect requirements and acquisition documents

Service/Agency Testing

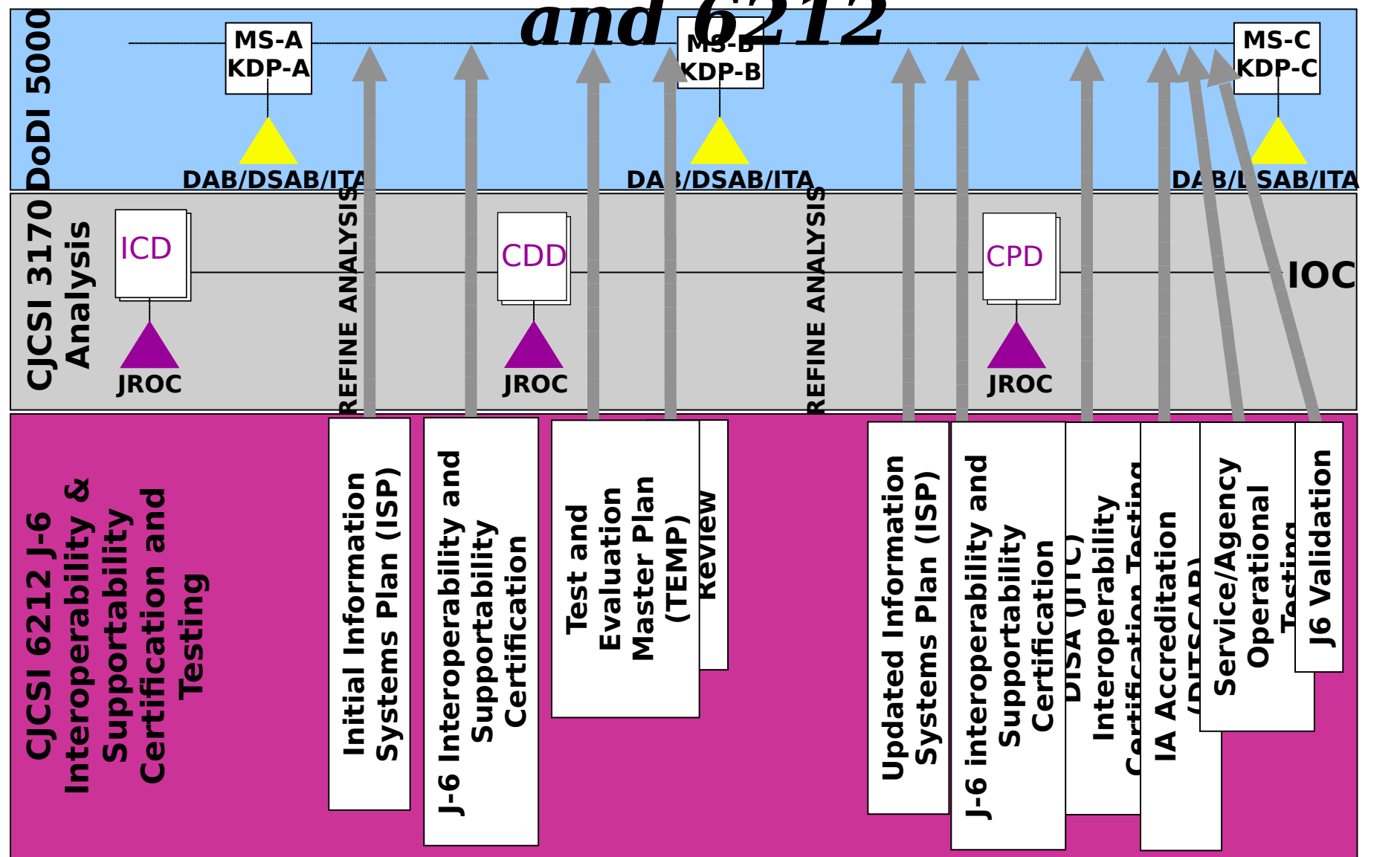
- DT/Standards Conformance
- OT&E
- Interoperability Testing

DISA(JITC) Interoperability Test Certification

J-6 Interoperability System Validation

Processes

Sync - DoDI 5000 & CJCSI 3170 and 6212



Interoperability KPP Today

Top-level IERs will be used as the basis to develop interoperability KPPs. The interoperability KPP definition will include that all top-level IERs will be satisfied to the standards specified in the threshold and objective values.

Typically the threshold criterion for the interoperability KPP will be 100 percent accomplishment of the critical top-level IERs, and the objective criterion for the interoperability KPP will be the accomplishment of all top-level IERs.

Interoperability KPP	Threshold (T)	Objective (O)
All top-level IERs will be satisfied to the standards specified in the Threshold (T) and Objective (O) values.	100% of top-level IERs designated critical	100% of top-level IERs

(CJCSI 6212.01B)

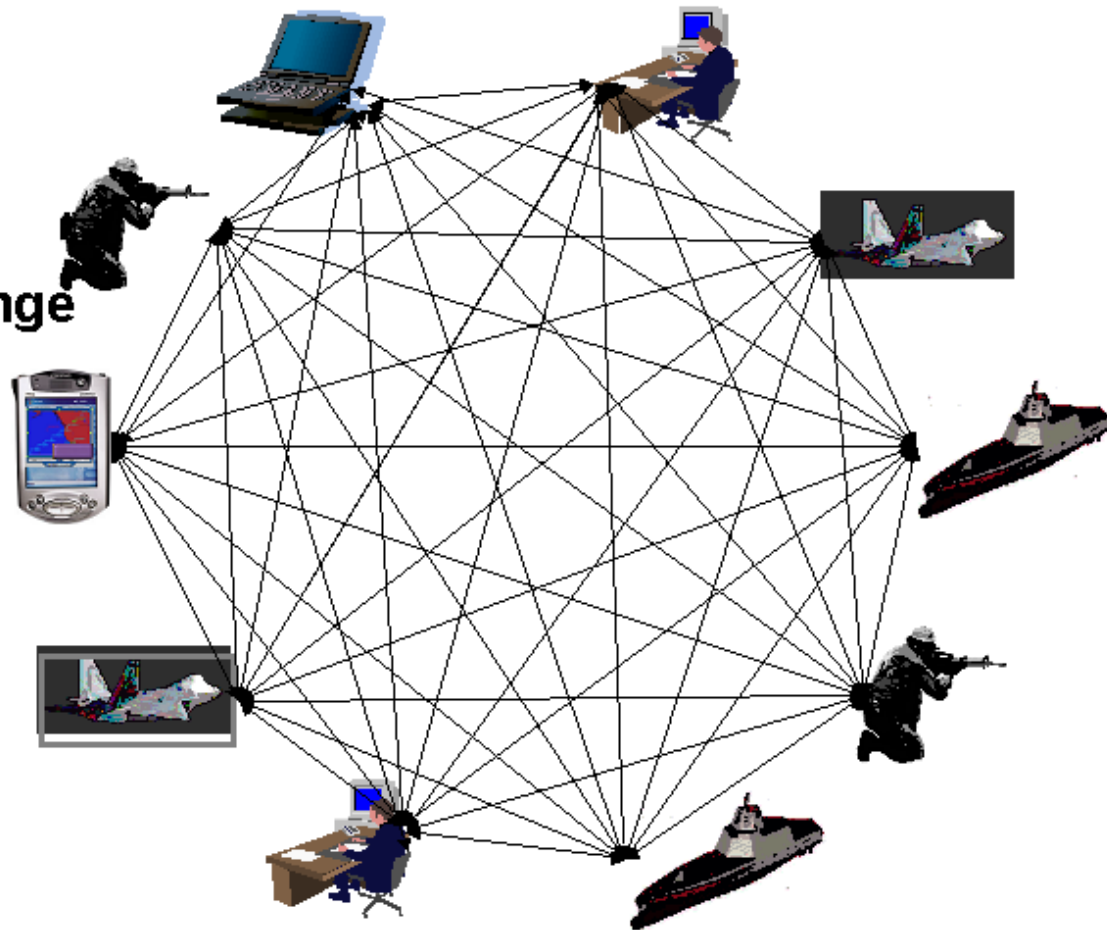
Problem: IER Scalability

One-to-One

Current Interoperability KPP centers around one DoD architectural view (OV-3) that contains “Information Exchange Requirements” (IERs)

- One-to-one relationship (point-to-point)

This example: 10 systems
IERs $10(9-1) = 90$



(OV-3) -Notional USCENTCOM Targeting Extract

* Identifier/ Name of Operational Needline Supported (from OV-2)	* Identifier/ Name of Information Exchange	Nature of Transaction								* Purpose/ Triggering Event	Information Source		Information Destination	
		* Mission/ Scenario	Language (For Multi-National Operations)	* Description (Content)	Size	Units	* Media	Collaborative (Y/N)?	LSI Level Required		* ID of Producing Node (facility or logical node)	* ID/ name of Producing Activity	* ID of Receiving Node (facility or logical node)	* ID/name of Receiving Activity
1	WOC-AOC	Targeting	Eng.	BDA Reports	1-10 pgs	.5-2 MB	.doc .jpg .img .ppt .gim	Y	2a	Air Strike 072200 0615am	XXXth TFW	WOC	609 AIS	AOC
	WOC-AOC	Targeting	Eng.	Target Nominations	1 pg	20KB	.doc	N	1b	ATO XXX 072300	XXXth TFW	WOC	609 AIS	AOC
2														
:	:	:	:	:	:	:	:	:	:	:	:	:	:	:
n	MAW-AOC	Targeting	Eng.	BDA Reports	1-10 pgs	.5-2 MB	.doc, .ppt .jpg, .gim .img	Y	2a	Air Strike 072200 0615am	VMF XXX	MAW	609 AIS	AOC

Note: All values shown above are notional.

Solution: The Net-Ready Approach

One-to-Many

Net Ready approach centers on central network:

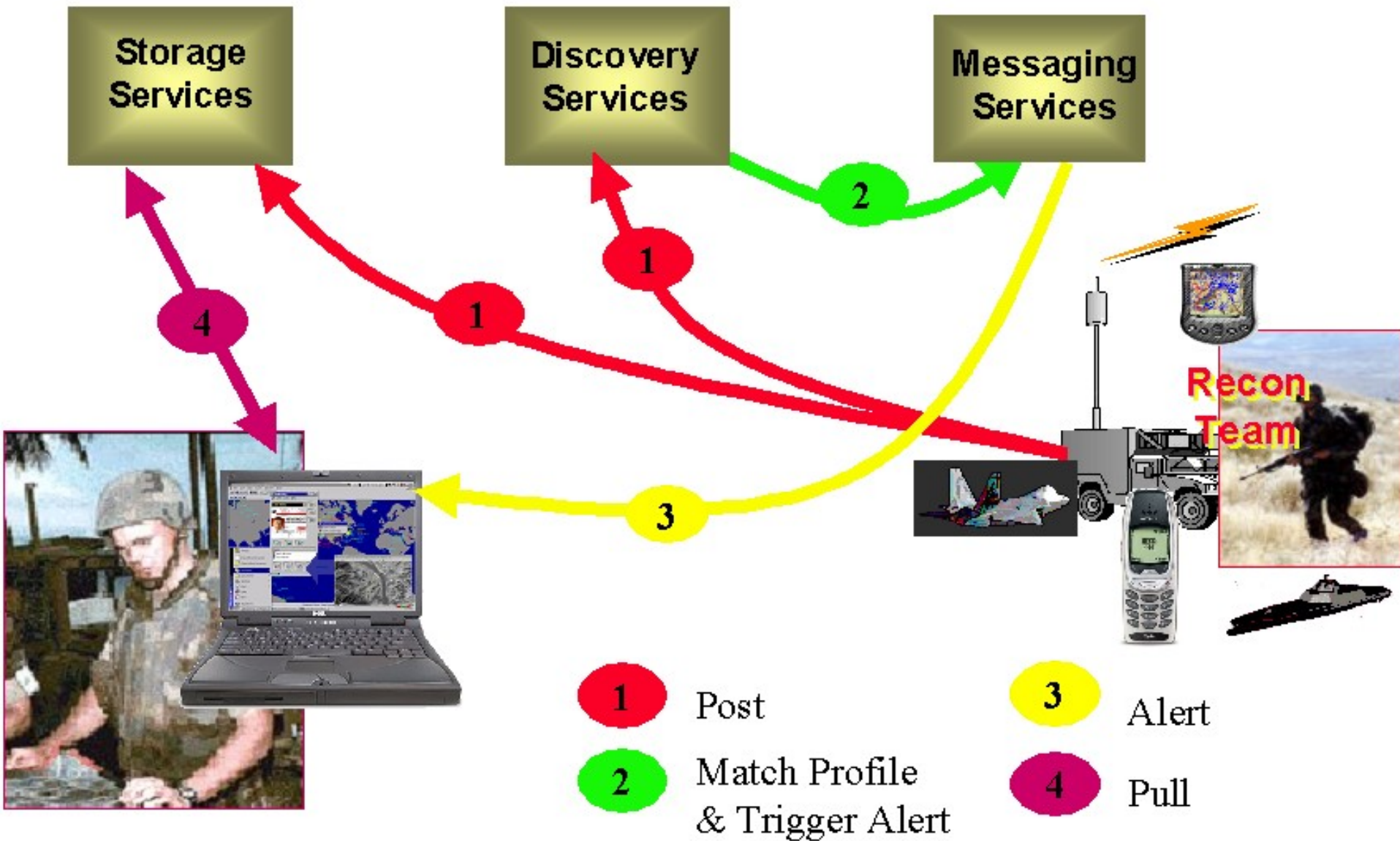
- **Focus on organizational contributions and consumption of information**
- **One-to-network paradigm**



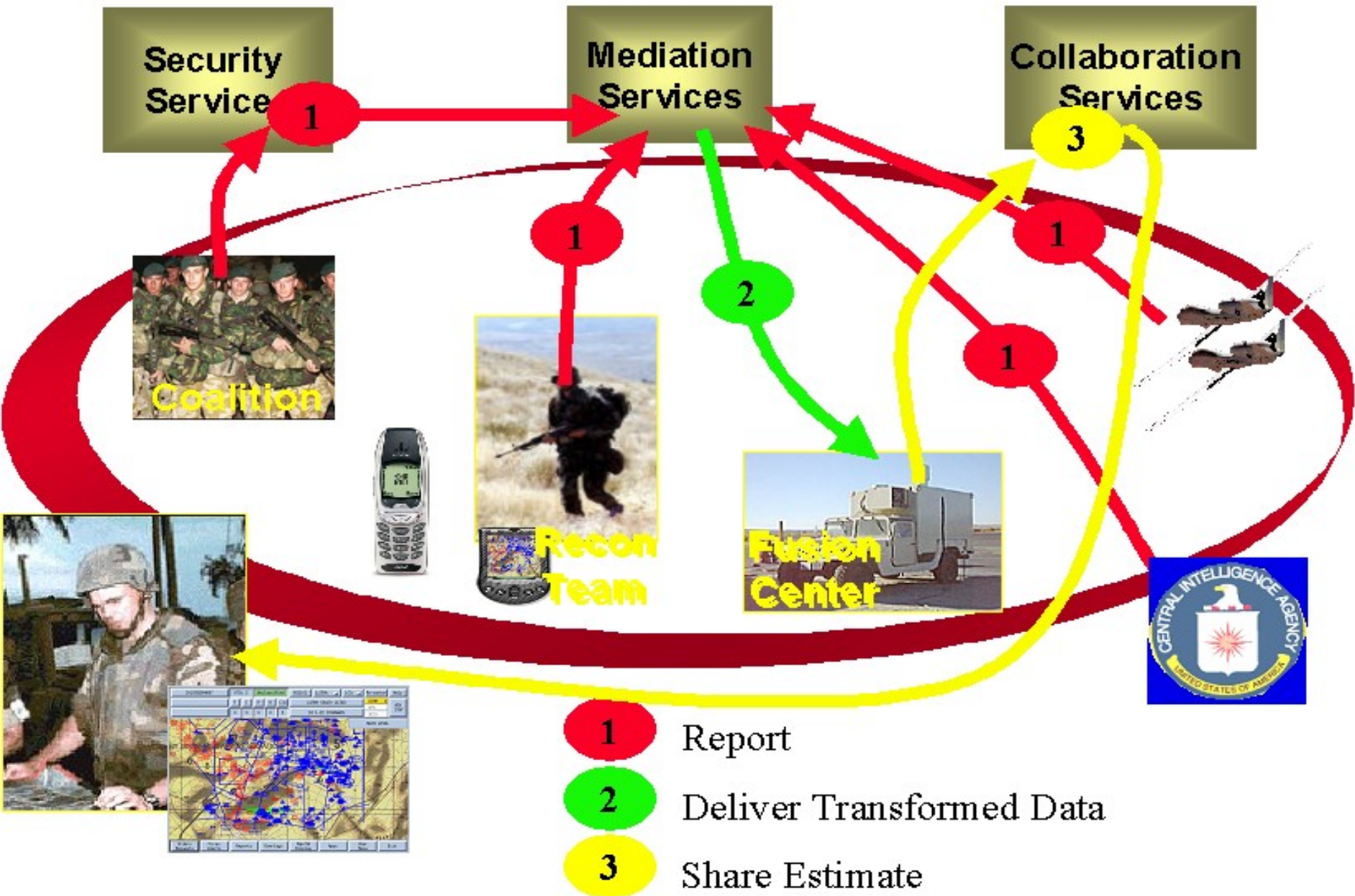
**This example: 1 system
has to deal 1 interface**



How GES/NCES works



How NCES works (Cont'd)

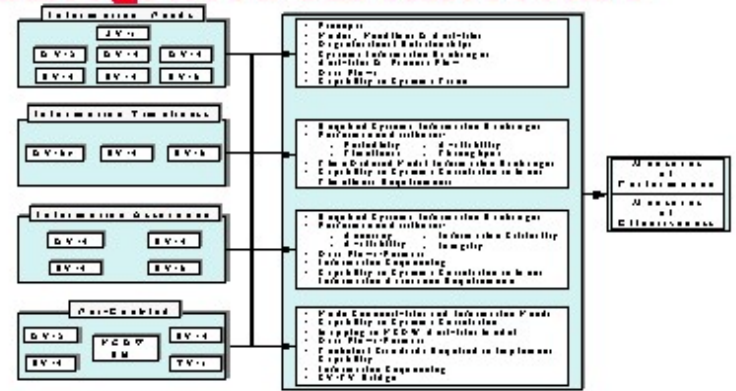


Net-Ready KPP

NCOW RM Compliance



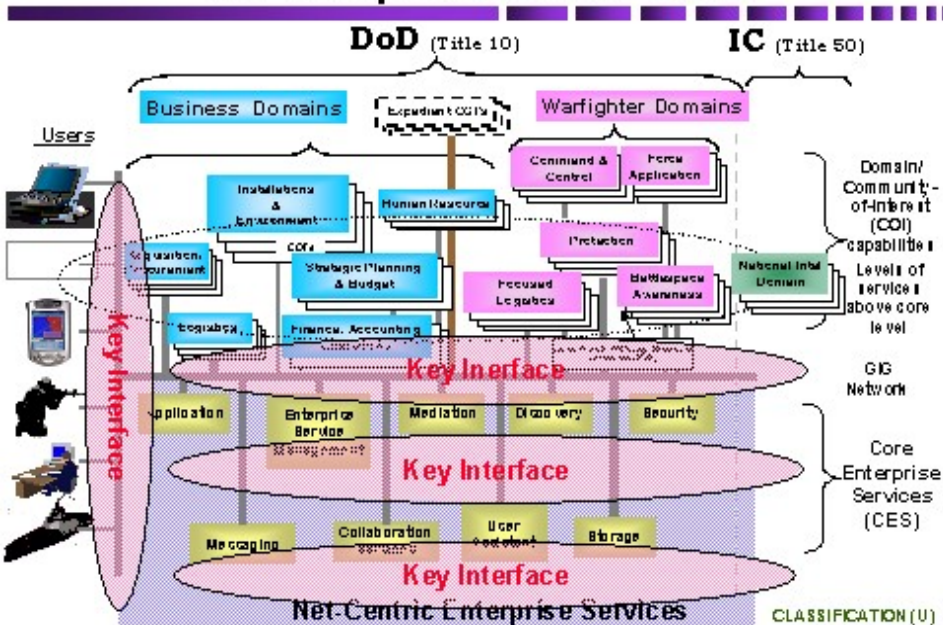
Integrated Architecture



KIP Compliance

CLASSIFICATION (U)

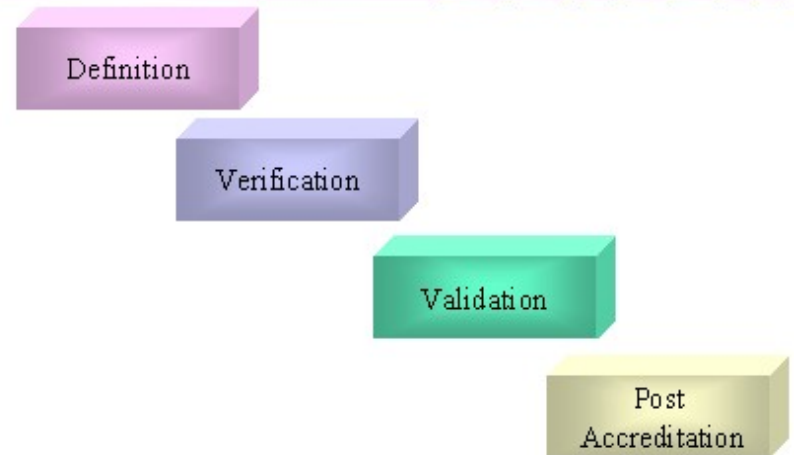
GIG Enterprise Services Vision



Information Assurance

CLASSIFICATION (U)

(DITSCAP*)
Information Assurance



*DoD Information Technology Security Certification and Accreditation Process

CLASSIFICATION (U)

Why Build a Reference Model?

- ✓ Provide Program Managers (the target audience) **acquisition guidance** on what to make contractually binding beyond the *Joint Technical Arch (JTA)*.
 - Provide immediate utility without time-consuming analysis of the DoD Enterprise Architecture (GIG Architecture Versions 1 and 2)
 - Overcome difficulty of relating and applying a broad Enterprise Architecture to specific programs.
- ✓ Provide **common net-centric architectural constructs** congruent with the DoDAF.
- ✓ Establish a **common language and taxonomy** for NCOW concepts.
- ✓ Demonstrate and promote the **TPPU Vision**.
- ✓ Focus the GIG Arch **compliance** requirement
- ✓ Support evolution of the *DoD Architecture Framework* and the *JTA*

Building the Model is a collective DoD effort

Reference Model Version 1.0 Content

Approved Dec 03

Overview and Summary Information

AV-1

NCOW REFERENCE MODEL
OVERVIEW AND SUMMARY INFORMATION

1. Identification

Name: NCOW Reference Model
BETA 2.0

Architect: OASD(NII), A&I

Organizations Involved:
xxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxx

When Developed:
xxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxx

2. Purpose
xxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Integrated Dictionary

AV-2

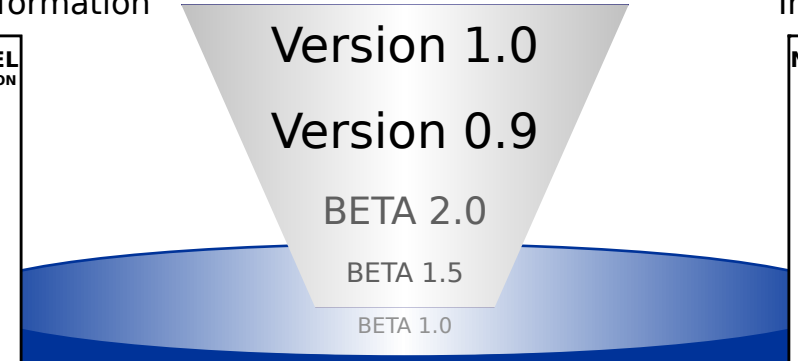
NCOW REFERENCE MODEL
INTEGRATED DICTIONARY

Kangaroo:
xxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxx

XXXXX:
xxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxx

XXXXX:
xxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxx

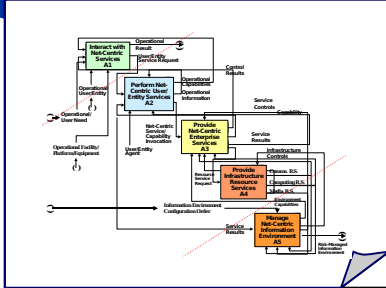
XXXXX:
xxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxx



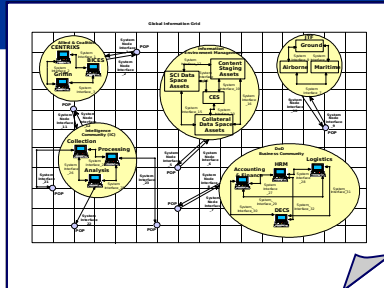
NCOW REFERENCE MODEL DATABASE



High-Level Operational
Concept Graphic
OV-1



Activity Model and
Activity Decomposition OV-
5



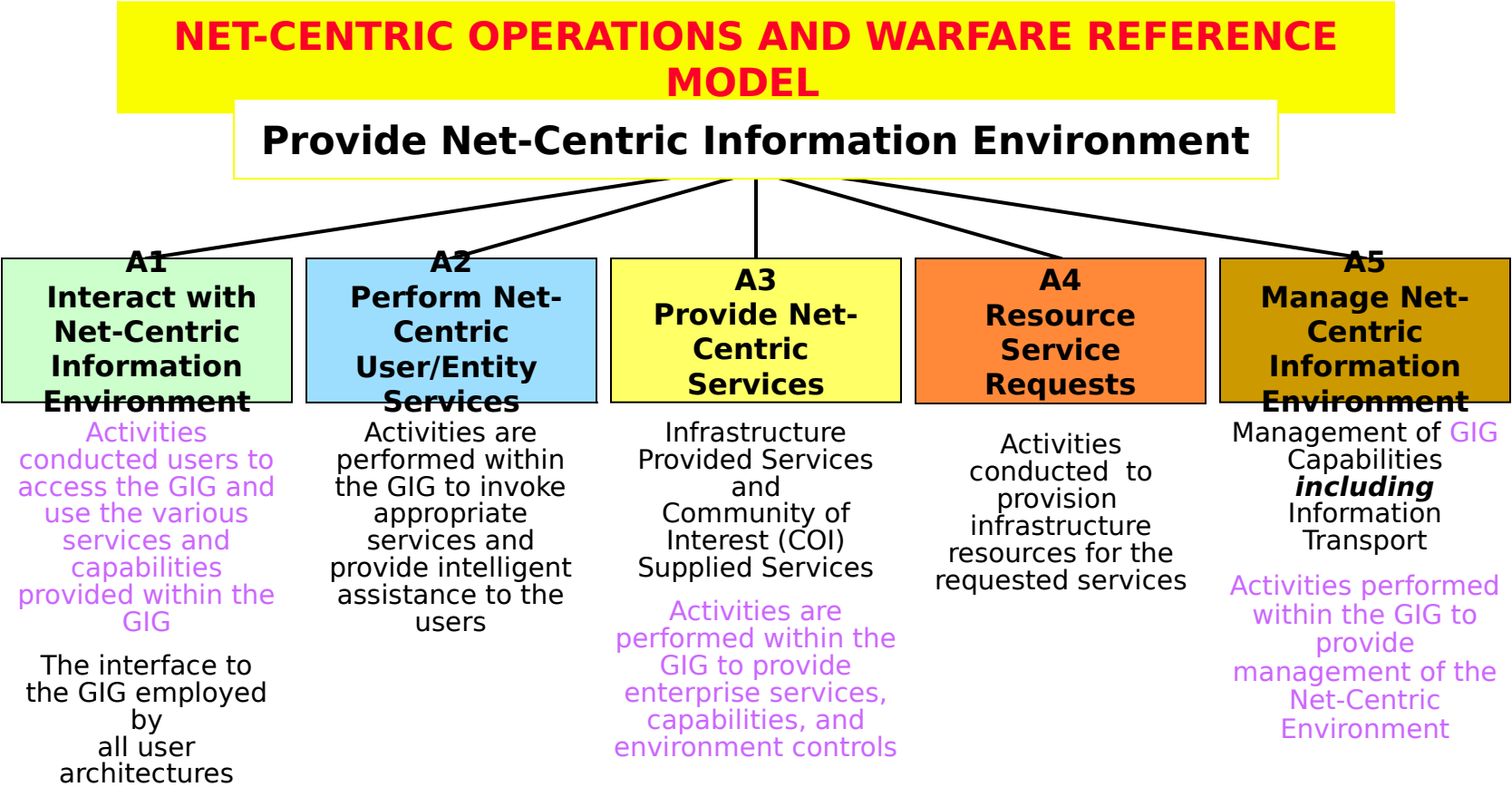
Systems View
SV-1 and SV-2

TECHNICAL SERVICE	STANDARD	OS LAYER
Directory Enabled Networking (DEN)	Directory Enabled Networking Protocol	Application 7
Common Open Relay Service (CORS)	CORS Protocol	Application 7
Common Information Mode (CIM)	CIM Policy Schemes	Application 7
Class of Service (COS)	Class Protocol	Network Routing 3
Routing Protocol Specification Language (RPSL)	RPSL Policy	Application 7
Internet Protocol (IP) Security Policy	IP Security Policy Protocol (IPSP)	Application 7
Service Level Agreement (SLA)	SLA Protocol on IP Network	Network Routing 3
Next Generation IP	Next Protocol	Application 7
Content Distribution and Management Storage Access Network	Network Data Management Protocol (NDMP)	Application 7
Universal Discovery Distribution Integration (UDDI)	UDDI Protocol	Presentation 6
Open Object Database Access	Simple Object Access Protocol (SOAP)	Presentation 6
Universal Web	Web Services Descriptive Language (WSDL)	Presentation 6
Bi-Directional IP Smart Pull in Broadcast Environment	Uni-Directional Link Routing Protocol (ULRP)	Link 2
Tag Switching for IP Routing	Multi-Protocol Label Protocol Switching (MPLS)	Transport 4
Mobile Ad hoc Networking (MANET)	MANET Protocol	Network Routing 3
Mobile Cryptography	None	
Integratable Intelligent Agent	None	
Integratable Aware Peer-to-Peer (IP2P) Protocol	None	
Scalability	None	
Survivability	None	

Target Technical
View

First description of Net-Centricity at the Enterprise Level

Reference Model Activity Decomposition



The diagram illustrates the Net-Centric Information Environment (NCIE) architecture, organized into five main functional areas (A0 through A4) and their associated tasks and capabilities.

A0: Provide Net-Centric Information Environment

- These activities are performed within the net-centric information environment to provide enterprise services, capabilities and environment controls.

A1: Interact with Net-Centric Services

- These are the activities conducted by a user to access the net-centric information environment and use the various services and capabilities provided by the environment.
- These activities are performed within the net-centric information environment to provide intelligent assistance to the user and resolve appropriate services.

A2: Perform Net-Centric User/Entity Services

- These activities are performed within the net-centric information environment to provide intelligent assistance to the user and resolve appropriate services.

A3: Provide Net-Centric Services

- These activities are performed within the net-centric information environment to provide intelligent assistance to the user and resolve appropriate services.

A4: Resource Service Requests

- These activities are performed within the net-centric information environment to provide intelligent assistance to the user and resolve appropriate services.

The diagram shows a hierarchical structure of tasks and capabilities, with A0 at the top, followed by A1, A2, A3, and A4. Each area is further subdivided into numerous specific tasks and capabilities, represented by colored boxes (green for A1, yellow for A2-A4, and red for A4). The diagram illustrates the flow of information and services from the user interface down to the underlying data and resource management layers.

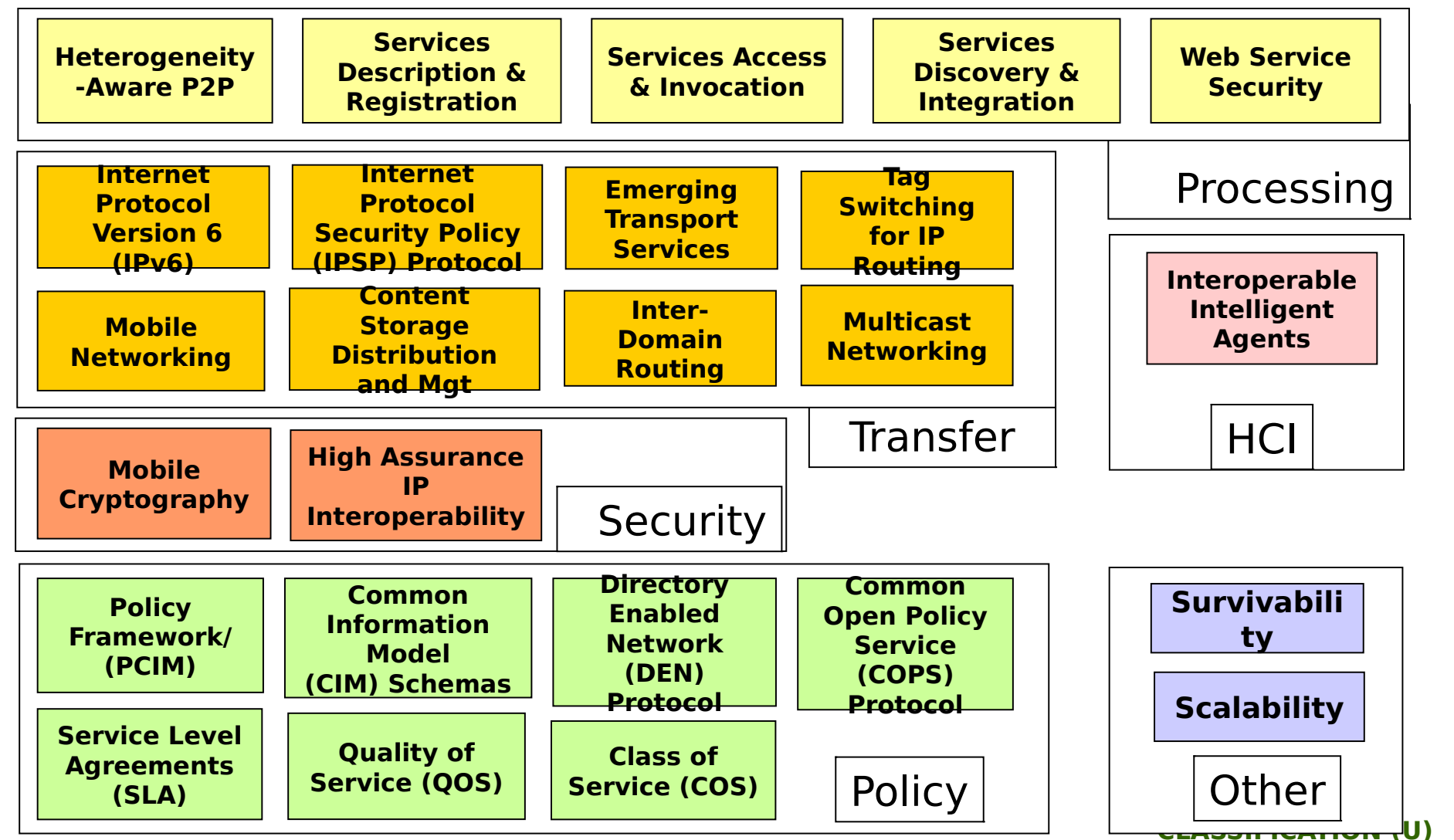
Perform
Net-Centric
User/Entity Services

Resource Service Requests

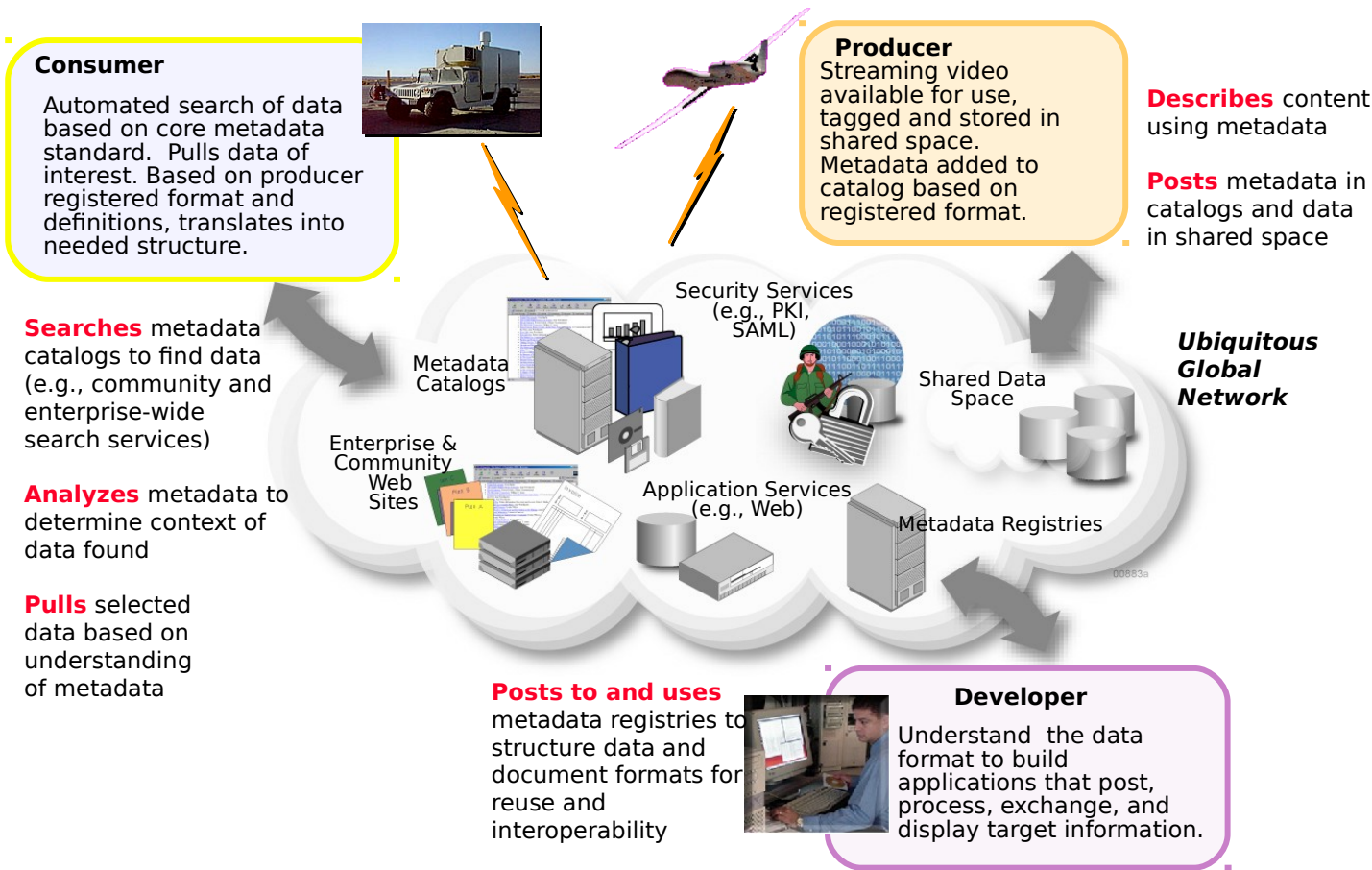
Manage Net-Centric Info Environment

NCOW RM Target Technical View

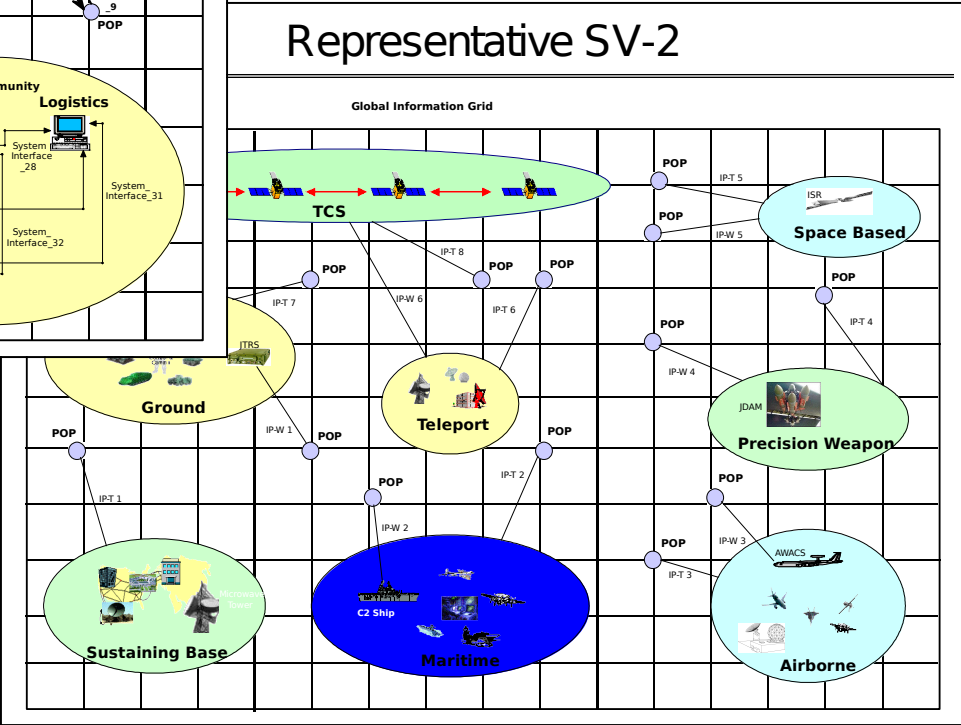
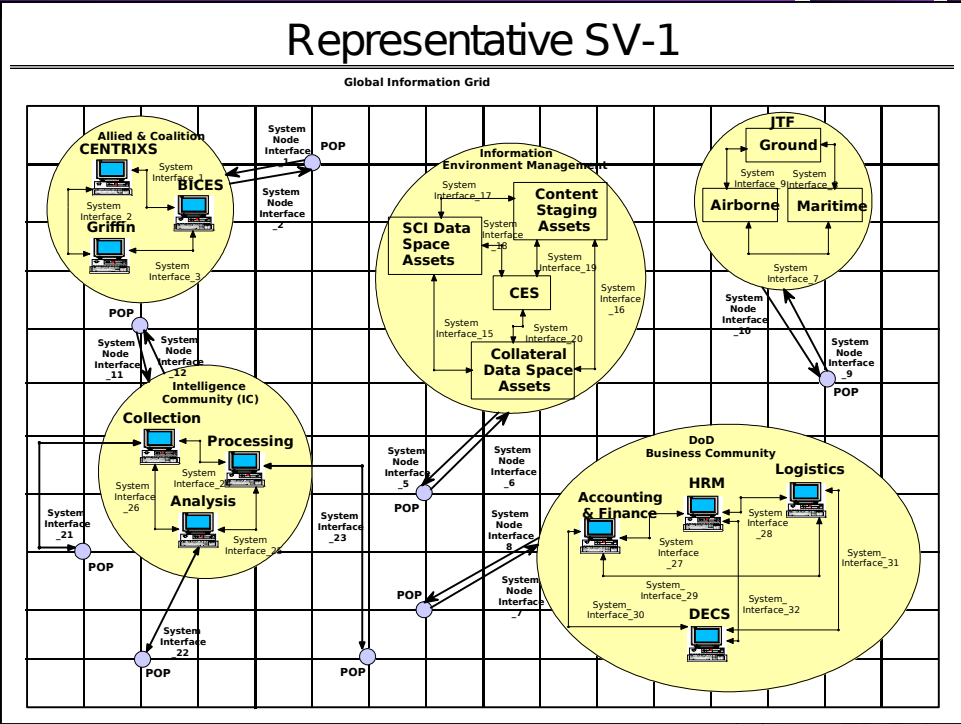
(Technical Areas by Core IT Category)



Net-Centric Data Strategy



Reference Model Systems View



Reference Model Versions

- Version 1.0
 - **Service Oriented Architecture**
 - **Approved Dec 03**
- Version 1.1
 - **Net-centric Data Strategy**
 - **DoD and Industry (NDIA) comments**
 - **Draft Version -- May 04**
- Version 1.2
 - **Net-centric Information Assurance Strategy**
 - **DoD and Industry (NDIA) comments**
 - **Draft Version -- July 04**

Net-centric Constructs

- Language/taxonomy
- Net-centric Service Oriented Architecture Strategy
- Net-centric Data strategy
- Net-centric Information Assurance Strategy

GIG Architecture Compliance

- ✓ Architecture products comply with **Architecture Framework** product definitions and purposes
 - ✓ Architecture data conform to the **CADM**
 - ✓ IT/NSS standards derived from the DoD **JTA** (or presents case for new or unique standards as necessary)
 - ✓ Conforms to the GIG **Net-Centric Operations and Warfare Reference Model:**
 - ✓ Uses Reference Model definitions and vocabulary
 - ✓ Incorporates Reference Model OV capabilities and services in the materiel solution
 - ✓ Net-centric SOA Strategy
 - ✓ Net-centric Data Strategy
 - ✓ Net-centric Information Assurance Strategy
 - ✓ Incorporated into the materiel solution
- Compliance is verified by inspection and analysis**

NCOW RM Conformance and Compliance



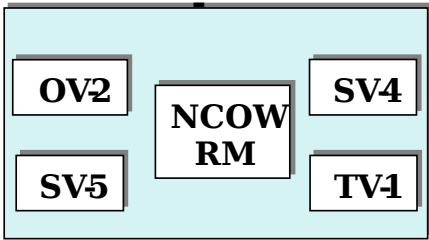
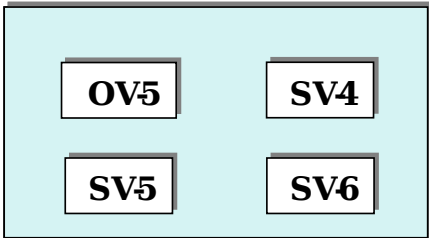
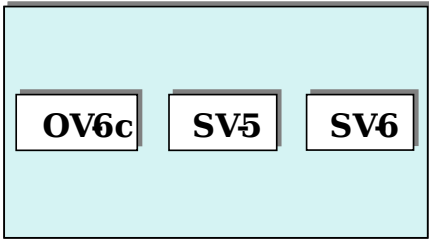
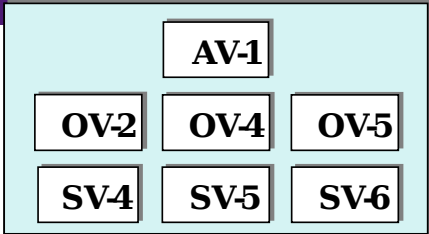
All DoD architectures are expected to comply and conform to the NCOW RM by:

- Using common NCOW RM definitions and vocabulary**
- Incorporating the capabilities and services described in the NCOW RM**
- Incorporating the IT/NSS standards identified in the NCOW RM**

This supports Compliance and conformance with the GIG translates to satisfying the requirements of the following five products:

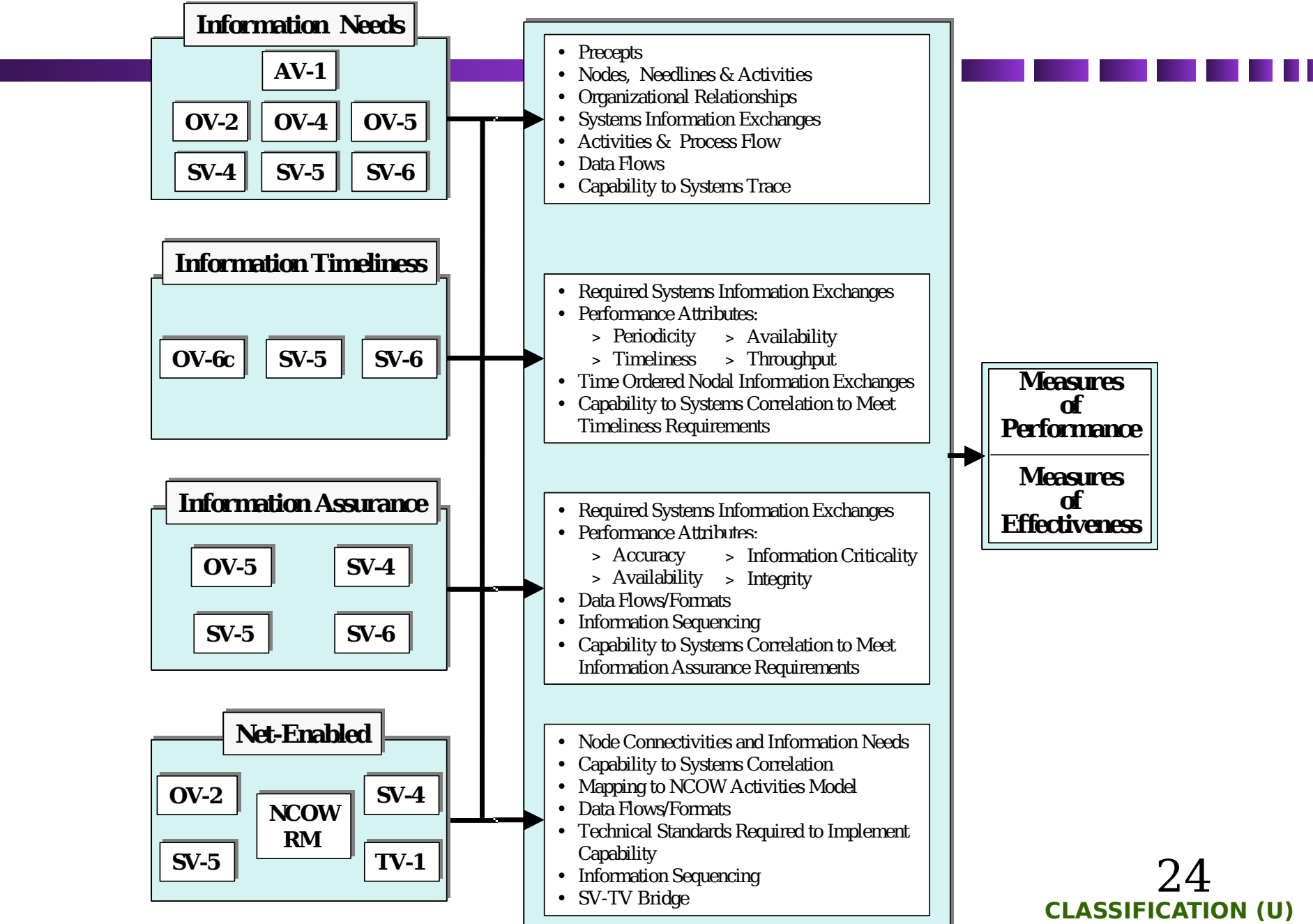
- DoD Architecture Framework (DoDAF)**
- Net-Centric Operations and Warfare Reference Model (NCOW RM).**
- Joint Technical Architecture (JTA) and the NCOW RM.**
- Core Architecture Data Model (CADM).**
- GIG Enterprise Services (GIG ES) Capability Description Document (CDD)**

Integrated Architecture



- **Operational Nodes**
- **Organizational Relationships**
- **Operational Activity**
- **Operational Event-Trace**
- **Systems Functionality Description**
- **Operational Activity to Systems Function**
- **Systems Data Exchange**
- **Technical Architecture Profile**

Integrated Architecture



Supporting Integrated Architecture Products

Framework Products	Framework Product Name	General Description
AV-1	Overview and Summary Information	Scope, purpose, intended users, environment depicted, analytical findings
OV-2	Operational Node Connectivity Description	Operational Nodes, operational activities performed at each node, connectivity and information exchange needlines between nodes
OV-4	Organizational Relationships Chart	Organizational, role, or other relationships among organizations
OV-5	Operational Activity Model	Operational activities, relationships among activities, inputs and outputs. Overlays can show cost performing nodes, or other pertinent information.
OV-6c	Operational Event-Trace Description	One of three products used to describe operational activity sequence and timing - traces actions in a scenario or sequence of events and specifies timing of
SV-4	Systems Functionality Description	Events performed by systems and the information flow among system functions
SV-5	Operational Activity to Systems Function Traceability Matrix	Mapping of systems back to operational capabilities or of system functions back to operational activities.
SV-6	Systems Data Exchange Matrix	Provides details of systems data being exchanged between systems.
TV-1	Technical Standards Profile	Extraction of standards that apply to the given architecture.

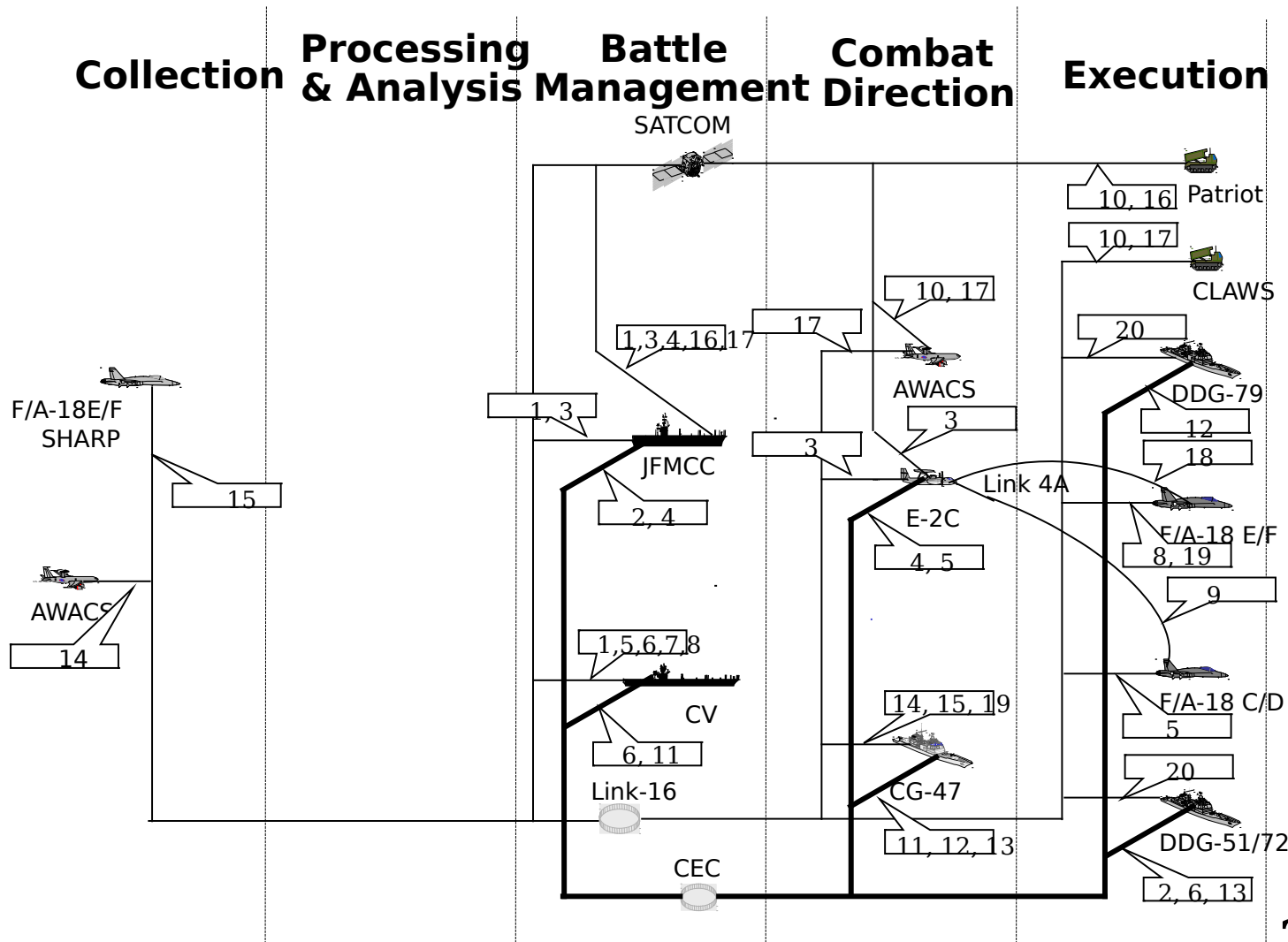
Architecture Analysis



Focus on Architecture and Standards.

- **First order analysis - identifying capability gaps, shortfalls and duplications.**
- **Second order analysis - identifies interoperability requirements.**

SV-1: 2003 Strike Mission Node Connectivity Diagram



Operational Activity to Systems Function Traceability Matrix (SV-5)



System Functions	Operational Activities																
	3.11	3.11.3	3.12	3.12.1	3.12.2	3.12.3	3.13	3.14	3.14.1	3.14.2	3.14.3	3.14.4	3.15	3.16	3.17	3.17.1	
1	X																
1.1		X															
1.1.1			X														
1.1.1.1	X																
1.1.1.2					X												
1.1.1.3						X											
1.1.2										X							
1.1.2.1				X													
1.1.2.2					X												
1.1.2.3								X									
1.1.3											X						
1.1.3.1													X				
1.1.3.2									X								
1.1.3.3														X			
1.1.3.4														X			

Systems Data Exchange Matrix (SV-6)

SV-6: 2003 Strike Mission (Illustrative Data)

IER No.	Sender	Receiver	Content	Media	Info Char	Format	Security	Freq	Timeliness	Thru put
1	JFMCC	CVIC	Target ID	JTIDS/SAT	Data	J 3.90	KG V-8	N/A	30 sec	N/A
2	DDG-51	JFMCC	Track Init.	DDS	Sensor	CEC data	KY-?	N/A	1 sec	N/A
3	JFMCC	E-2C	Engage Order	JTIDS/SAT	Data	J 13.85	KG V-8	N/A	15 sec	N/A
4	E-2C	JFMCC	Track Update	DDS	Sensor	CEC data	KY-?	N/A	7ms	N/A
5	CVIC	F/A-18	Engage Order	JTIDS	Data	J 13.85	KG V-8	N/A	10ms	N/A
6	DDG-51	CVIC	Target Loc	DDS	Sensor	CEC data	KY-?	N/A	4 sec	N/A
7	Patriot	CVIC	Target Acq	JTIDS	Data	J 4.56	KG V-8	N/A	2 min	N/A
8	F/A-18CD	CVIC	Target Killed	JTIDS	Data	J 8.76	KG V-8	N/A	3 min	N/A
9	E-2C	CVIC	CAP Posit	JTIDS	Data	J 10.74	KG V-8	N/A	35 sec	N/A
10	Patriot	AWACS	Target Loc	JTIDS/SAT	Data	J 12.101	KG V-8	N/A	4 Sec	N/A
11	CG-47	CVIC	Target Loc	DDS	Sensor	J 12.101	KY-?	N/A	2 sec	N/A
12	CG-47	DDG-81	Target ID	DDS	Sensor	CEC data	KY-?	N/A	1 sec	N/A
13	DDG-51	CG-47	Posit Info	DDS	Sensor	CEC data	KY-?	N/A	500 ms	N/A
14	CG-47	AWACS	Cse Orders	JTIDS	Data	J 7.99	KG V-8	N/A	2 min	N/A
15	CG-47	SHARPS	Cse Orders	JTIDS	Data	J 7.99	KG V-8	N/A	2 min	N/A
16	Patriot	JFMCC	Target Loc	JTIDS/SAT	Data	J 12.101	KG V-8	N/A	4 min	N/A
17	Hawk	JFMCC	Target Loc	JTIDS/SAT	Data	J 12.101	KG V-8	N/A	4 min	N/A
18	E-2C	F/A-18EF	Cse Orders	JTIDS	Data	FDL	KG V-8	N/A	30 sec	N/A
19	F/A-18EF	CG-47	Target ID	JTIDS	Data	J 3.90	KG V-8	N/A	30 sec	N/A
20	DDG-81	DDG-51	Target ID	JTIDS	Data	J 3.90	KG V-8	N/A	30 sec	N/A

Note: Notional architecture for instructional purposes

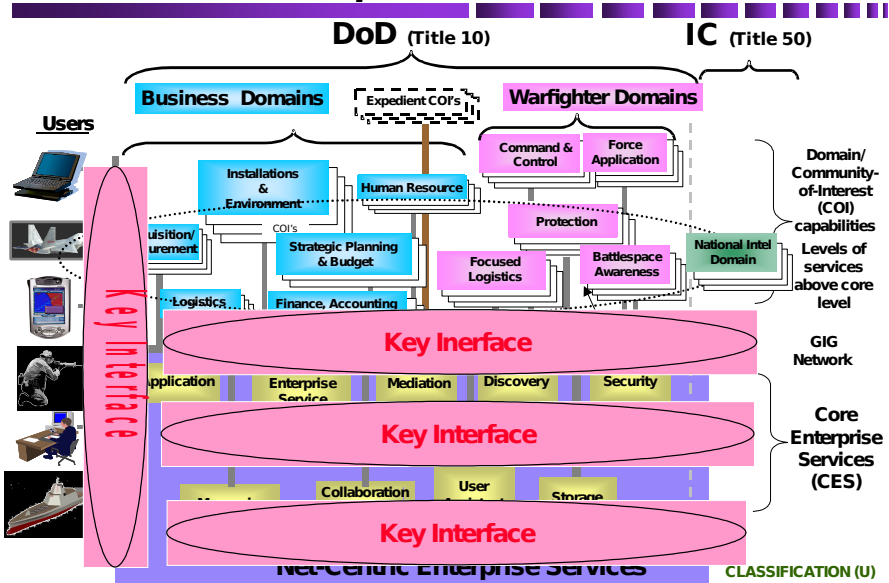
Key Interface

Net-Centric Operations and Warfare (NCOW) Reference Model
Operational Concept Graphic (OV-1a)

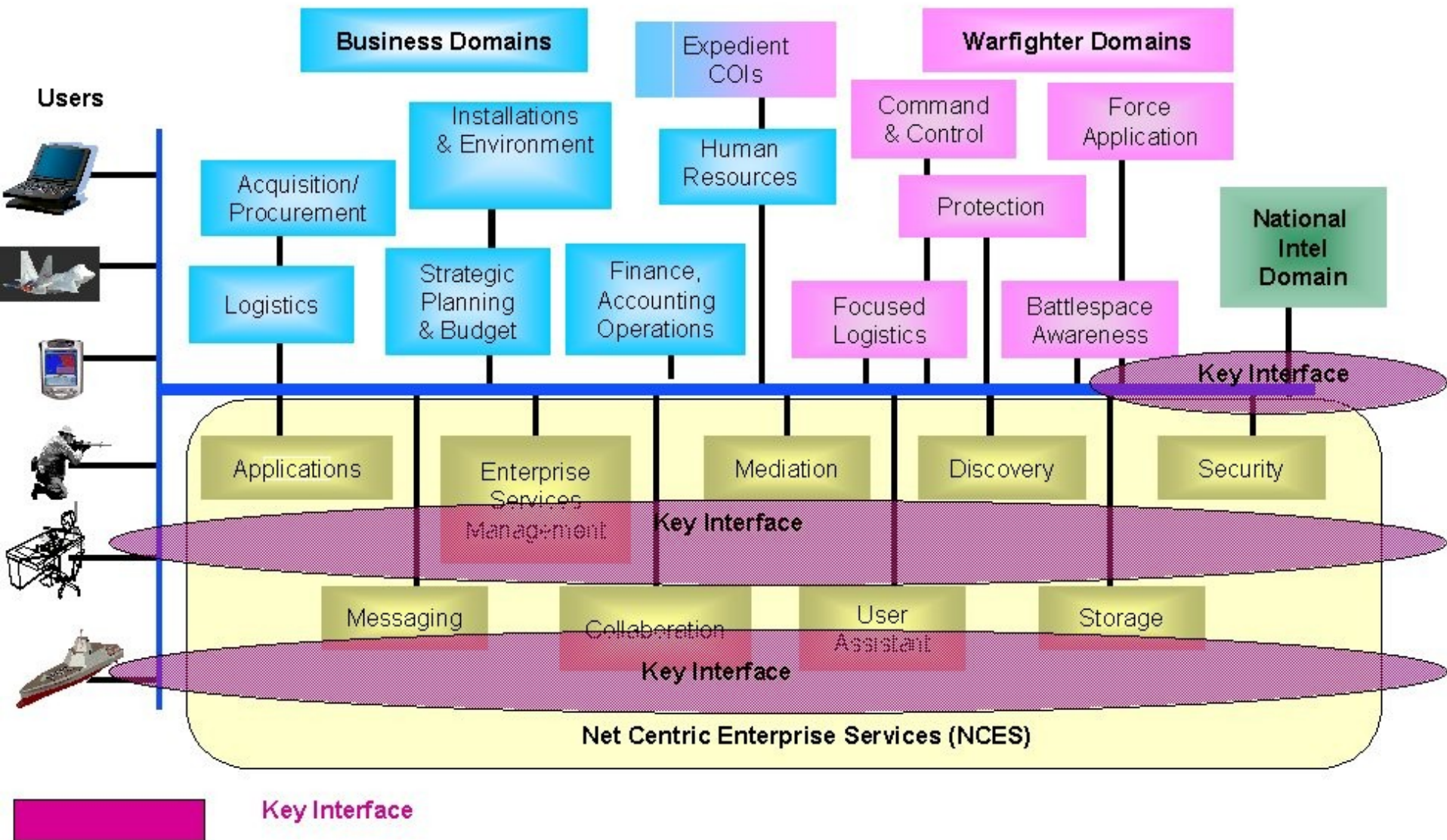


- Organizational boundaries.
- Mission critical.
- Difficult or complex to manage.
- Capability, interoperability, or efficiency issues.
- Impacts multiple acquisition programs.
- Vulnerable

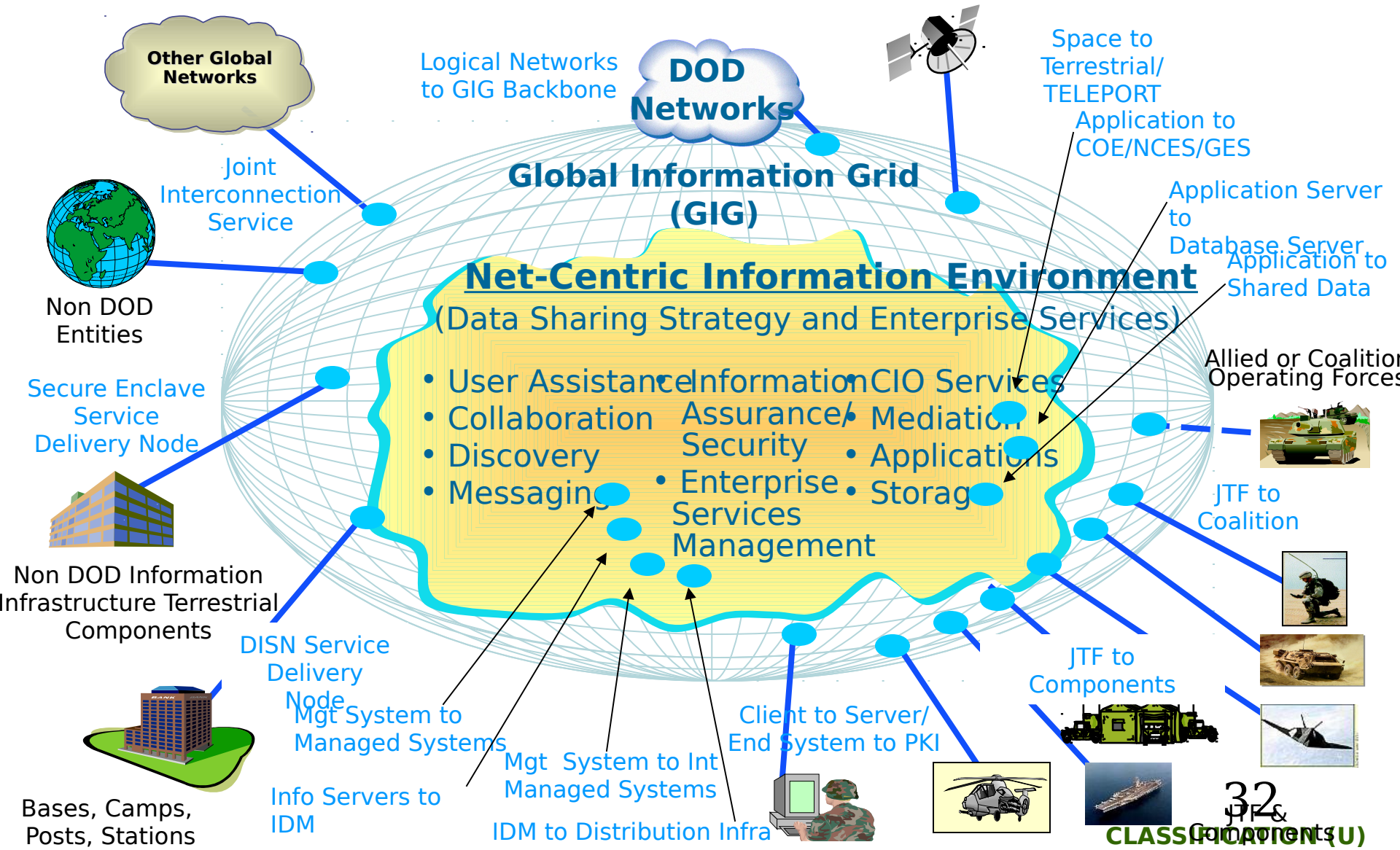
GIG Enterprise Services Vision



GES/NCES



KIPs to NCES/GES



The 17 Key Interfaces



Communications KIPs

- Logical Networks to DISN Transport Backbone
- Space to Terrestrial Interface
- JTF to Coalition
- JTF Component to JTF Headquarters
- Teleport** (i.e., deployed interface to DISN)
- Joint Interconnection Service
- DISN Service Delivery Node
- Secure Enclave Service Delivery Node (e.g., **SCI/Collateral KIP**)

Computing KIPs

- Application Server to Database Server
- Client to Server
- Applications to COE/CCP

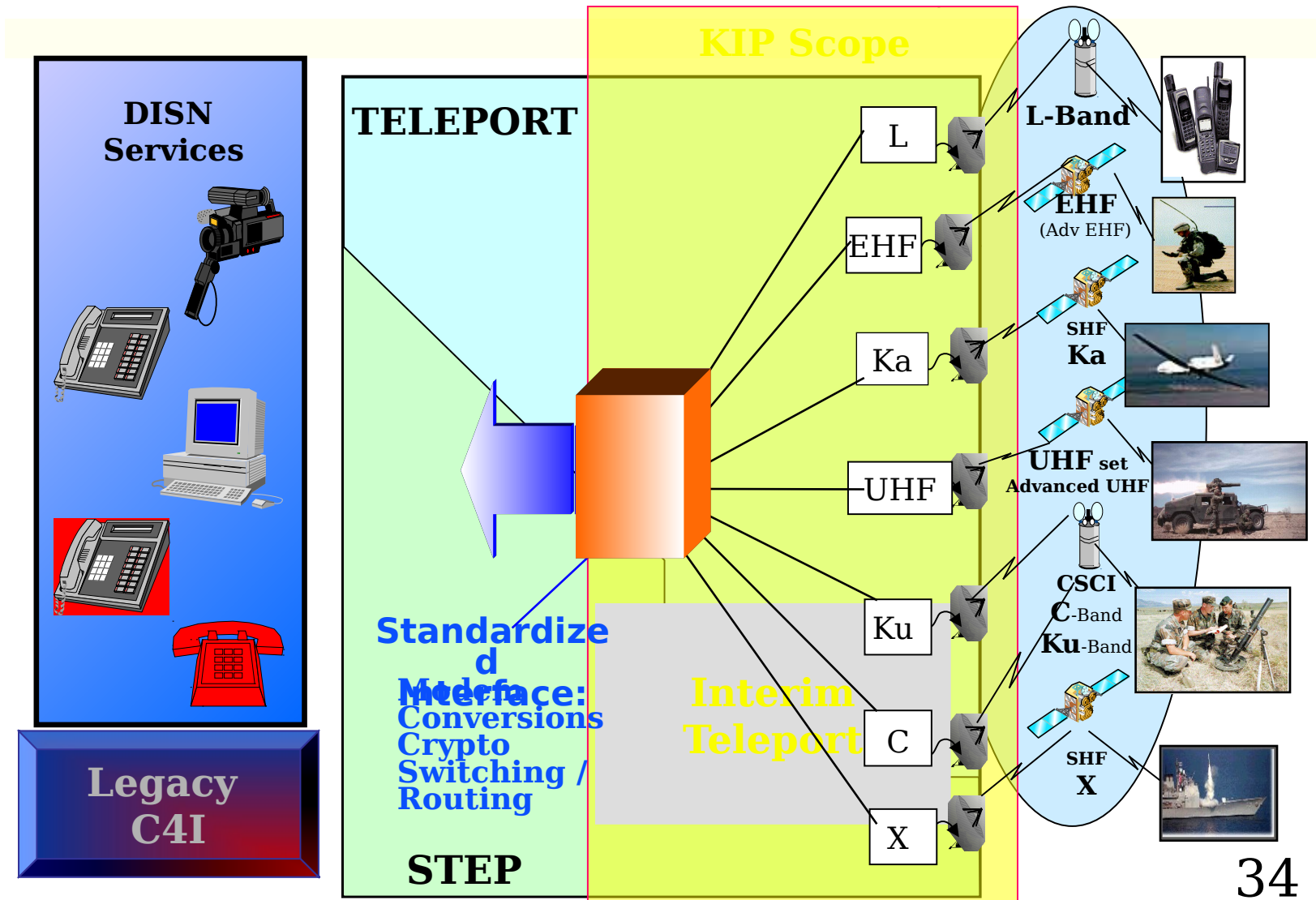
Network Operations KIPs

- End System to PKI
- Management Systems to (integrated) Management Systems
- Management Systems to Managed Systems
- IDM to Distribution Infrastructure
- Information Servers to IDM Infrastructure

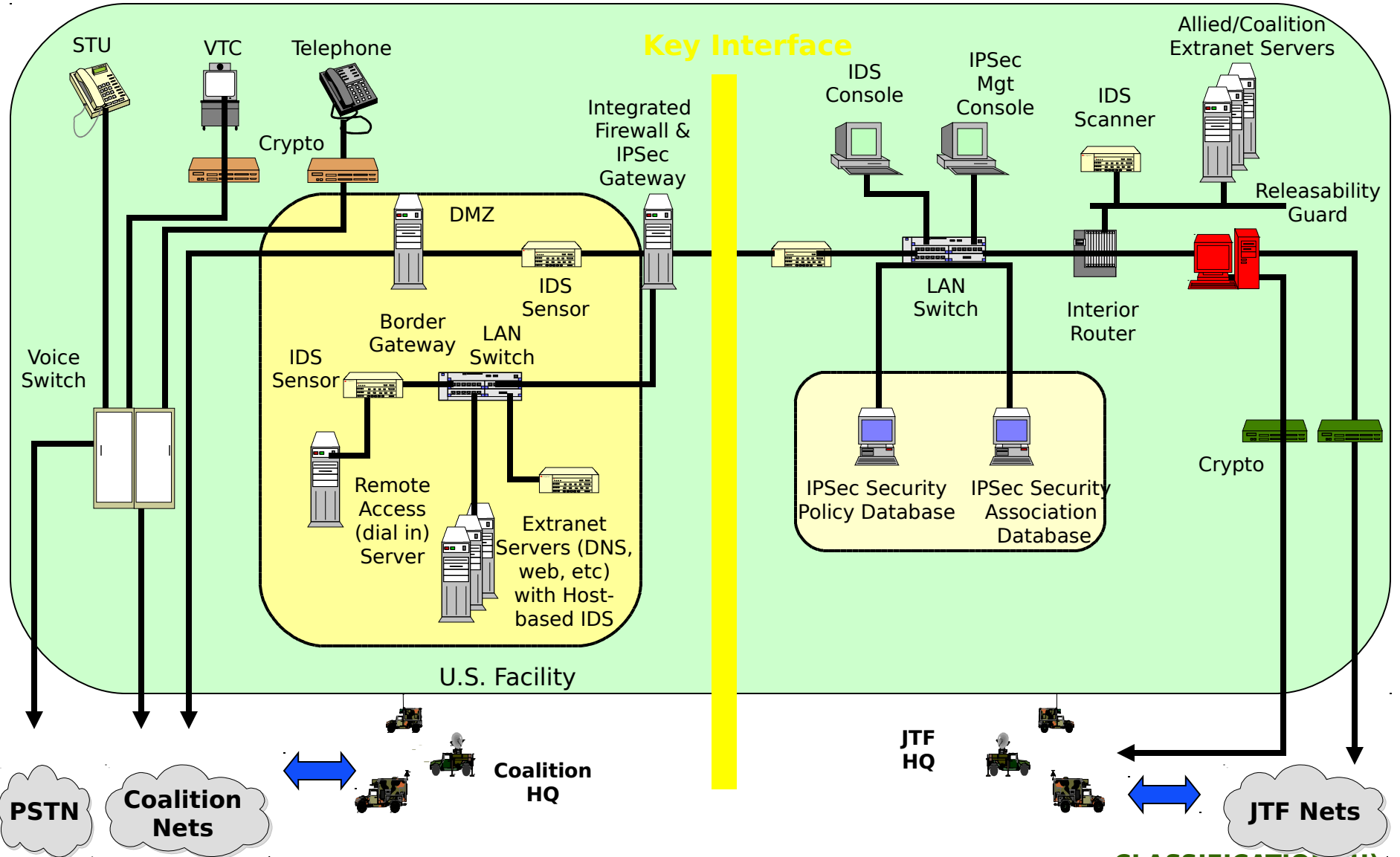
Applications

- Application Server to Shared Data (e.g., **Situational Awareness Data KIP**)
- (Pilot Projects in Red)**

STEP/TELEPORT



JTF to Coalition



Key Interface Profile

- 
- ✓ **Refined Operational View**
 - ✓ **Refined System View**
 - ✓ **Interface Control Specifications -- Interface Control Document (ICD)**
 - ✓ **Technical View & SV-TV Bridge**
 - ✓ **Configuration Management Plan**
 - ✓ **Procedures for Standards Conformance and Interoperability Testing utilizing reference implementations**
 - ✓ **Engineering Management Plan**

KIP Analysis

- **Logical Networks to DISN Transport Backbone.** Does your network connect to DISN Backbone?
- **Space to Terrestrial.** Does your ground terminal utilize or require access to DOD SATCOM programs such as DSCS, MILSTAR, FLTSAT, UFO, MUOS, Polar EHF, GPS, GBS, INMARSAT, Wideband Gapfiller, etc?
- **STEP and TELEPORT.** Does your ground terminal interface with/connect with STEP/TELEPORT systems?
- **JTF to Coalition.** Does your program or system interface with/connect the JTF to coalition forces?
- **JTF Component to JTF Headquarters.** Does your program or system interface/connect the JTF Component to the JTF Headquarters?
- **Joint Interconnection Service.** Does your organization connect the NIPRNET to Internet?
- **DISN Service Delivery Point.** Does your base, camp, post, station, unit or organization connect to the DISN?
- **Secure Enclave Service Delivery Point.** Does your system or program interface with or connect a Secure Enclave local area network to DISN service delivery point?
- **Client to Server.** Does your workstation publish, utilize or require access to data residing in DOD/NCES/GES servers?
- **End System to PKI.** Do your workstation and applications utilize or interface with utilize DOD **PKI**?
- **Information Servers to IDM Infrastructure.** Does your information server (collaboration, discovery, mediation, security, application, messaging, etc) require access to NCES/GES Infrastructure?
- **IDM to Distribution Infrastructure.** Does your network management system and communications system requires access to NCES/GES?
- **Management Systems to Managed Systems.** Does your system for personal and local computing manage the local network infrastructure (routers, WAPs, switches, hubs, firewalls, gateways, IDS), servers, and terminal devices (desktop computers, printers, wireless terminals)?
- **Management Systems to (Integrated) Managed Systems.** Does your management system interface with DOD GNOSC, RNOSC? Includes NIPRNET NOC, GSSC, SIPRNET NOC, DSN NOC, DRSN NOC?
- **Applications Server to Database Server.** Does your web or application server require access to NCES/GES database server(s)?
- **Applications to Shared Data.** Does your application require access to shared data residing in NCES/GES infrastructure?
- **Application to COE/NCES/GES.** Does your application require access to COE/NCES/GES services?

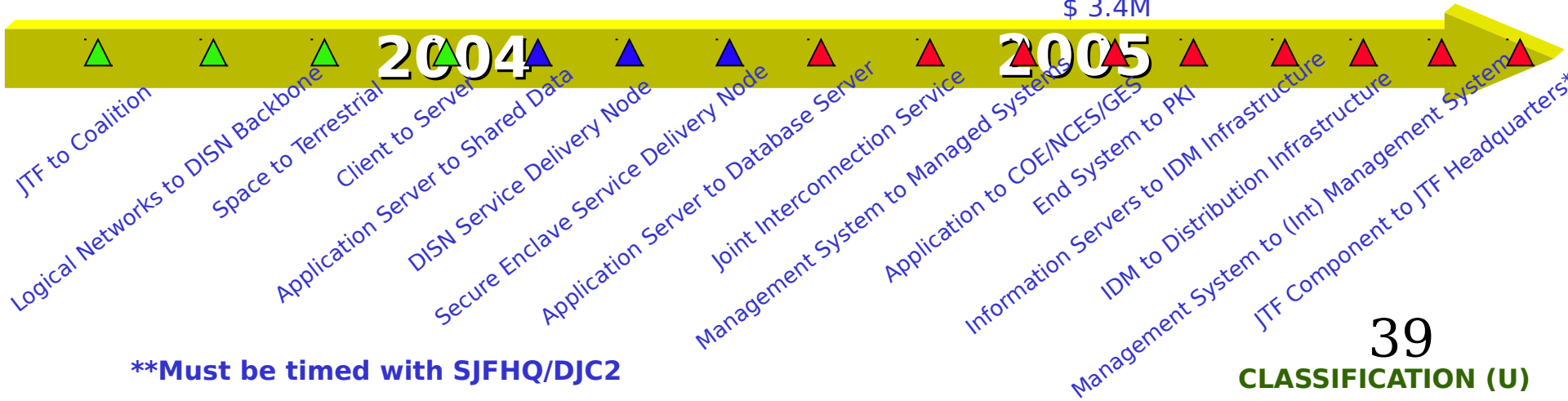
KIP Compliance



- **Analysis required by PM to determine applicable KIPs**
- **Implemented IAW profile**
- **Validated during testing**

Key Interfaces - Prioritized/Funding Requirements

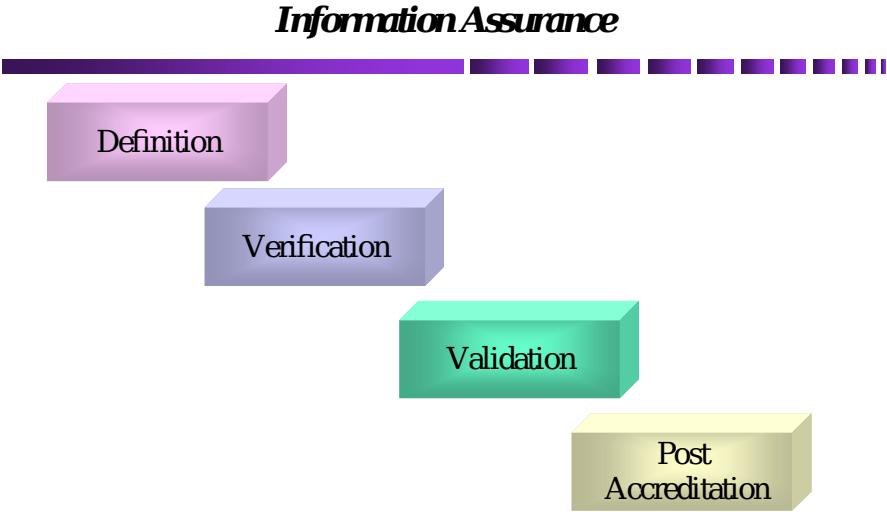
Priority	Key Interface Profile	Estimated Cost
1.	JTF Component to JTF Headquarters**	400K
2.	JTF to Coalition	300K
3.	Logical Networks to DISN Transport Backbone.....	100K
4.	Space to Terrestrial	300K
5.	TELEPORT.....	done
6.	Client to Server	100K
7.	Application Server to Shared Data	50K
8.	DISN Service Delivery Node	200K
9.	Secure Enclave Service Delivery Node	250K
10.	Application Server to Database Server	200K
11.	Joint Interconnection Service	200K
12.	Management System to Managed Systems	250K
13.	Application to COE/CCP (NCES/GES)	200K
14.	End System to PKI	200K
15.	Information Servers to IDM Infrastructure	250K
16.	IDM to Distribution Infrastructure	200K
17.	Management System to (integrated) Management Systems	<u>200K</u>
		\$ 3.4M



****Must be timed with SJFHQ/DJC2**

Information Assurance (DITSCAP*)

CLASSIFICATION (U)



- Availability
- Integrity
- Authentication
- Confidentiality
- Non-repudiation

CLASSIFICATION (U)

INFORMATION ASSURANCE (IA): Information Operations that protect and defend information and information systems by ensuring their **availability, integrity, authentication, confidentiality, and non-repudiation.**

*DoD Information Technology Security Certification and Accreditation Process

Certification and Accreditation Process (DITSCAP)

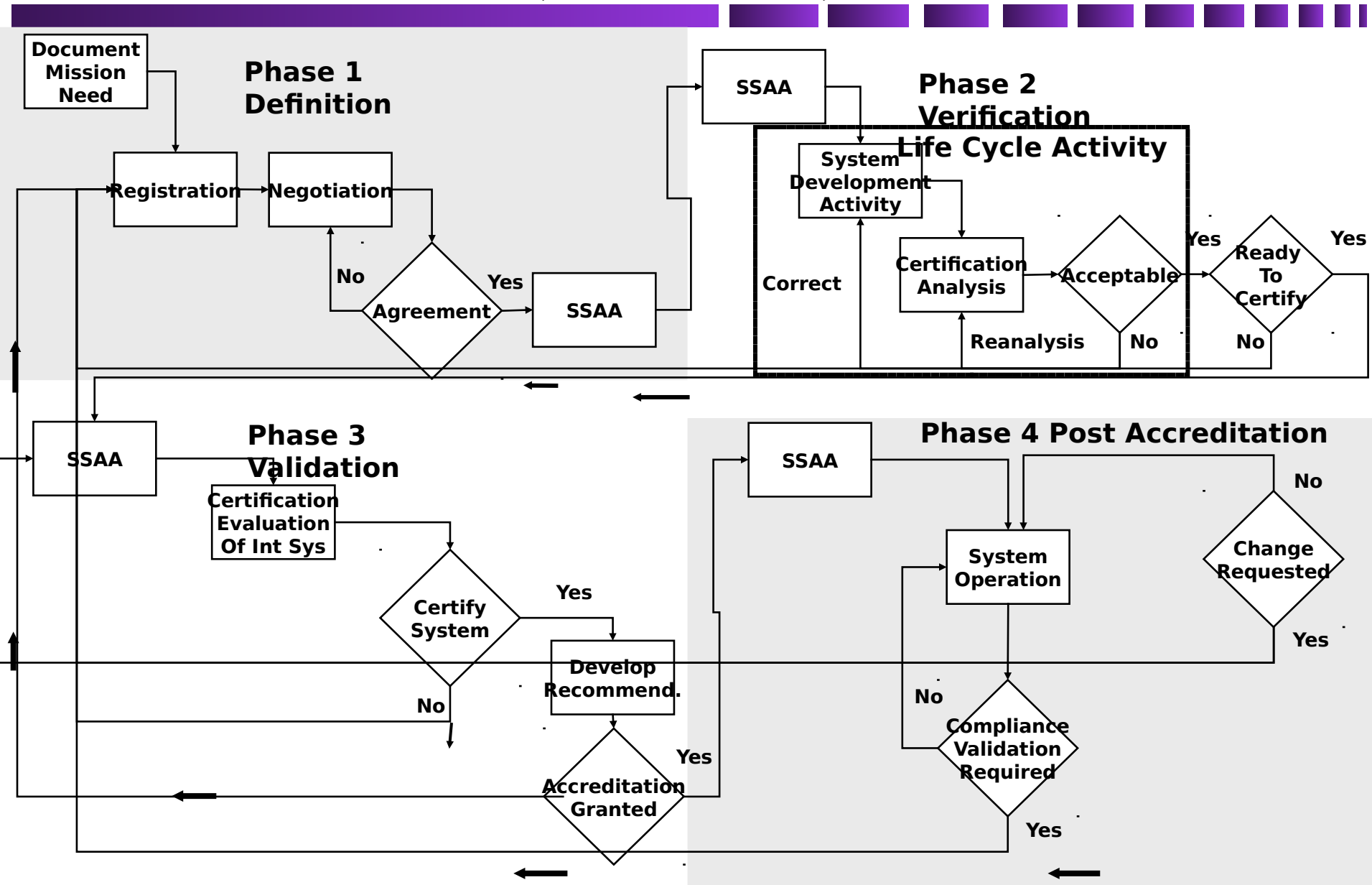


Table E4-1. Management Responsibilities by DITSCAP Phase.

Phase	Program Manager	DAA and CA	User Representative
Phase 1	Initiate security dialogue with DAA, the CA, and the user representative. Define system schedule and budget. Define and/or validate system performance, availability, and functionality requirements. Support DITSCAP tailoring and level of effort determination. Draft or support drafting of the SSAA. Reach agreement on the SSAA. Approve the SSAA.	Define ITSEC accreditation requirements. Obtain threat assessment. Begin vulnerability and risk assessments. Assign the CA. Support DITSCAP tailoring and determine the level of effort. Draft or support drafting of the SSAA. Reach agreement on the SSAA. Approve the SSAA.	Validate and/or define system performance, availability and functionality requirements. Support DITSCAP tailoring and level of effort determination. Reach agreement on the SSAA. Approve the SSAA.
Phase 2	Review the SSAA. Develop system or system modifications. Support certification actions. Review certification results. Revise system as applicable.	Review the SSAA. Evaluate developing system. CA performs certification actions. CA assesses vulnerabilities. CA reports results to the program manager, the DAA, and the user representative. Maintain the SSAA.	Review the SSAA. Support certification actions. Support certification actions.

Table E4-1. Management Responsibilities by DITSCAP Phase.

Phase	Program Manager	DAA and CA	User Representative
Phase 3	Review the SSAA. Test integrated system. Support certification actions. Review certification results. Revise system as applicable. Support SSAA revisions.	Review the SSAA. Evaluate developing system. CA performs certification actions. Assess vulnerabilities and residual risk. CA reports results to the program manager, the DAA, and the user representative. CA develops recommendation to the DAA. CA prepares accreditation package. Review the SSAA. Issue decision.	Review the SSAA. Support certification actions. Review certification results. Support SSAA revisions.
Phase 4	Review SSAA periodically. Operate system as described in the SSAA. Maintain an acceptable level of residual risk. Submit proposed changes to the user representative, the ISSO, the DAA, and the CA, as applicable. Support compliance validation.	Review the SSAA. Review proposed changes Oversee compliance validation.	Review the SSAA. Oversee system operation as described in the SSAA. Maintain an acceptable level of residual risk. Continuously review threat, system vulnerabilities and residual risk. Review and approve proposed changes. Submit significant changes to the DAA and the CA. Perform compliance validation actions.

Net Ready KPP Statement

Net Ready KPP	Threshold (T)	Objective (O)
All activity interfaces, services, policy-enforcement controls, and data-sharing of the NCOW-RM and GIG-KIPs will be satisfied to the requirements of the specific Joint integrated architecture products (including data correctness, data availability and data processing), and information assurance accreditation, specified in the threshold (T) and objective (O) values.	100% of interfaces; services; policy-enforcement controls; and data correctness, availability and processing requirements designated as enterprise-level or critical in the Joint integrated architecture	100% of interfaces; services; policy-enforcement controls; and data correctness, availability and processing requirements in the Joint integrated architecture

JROCM Guidance

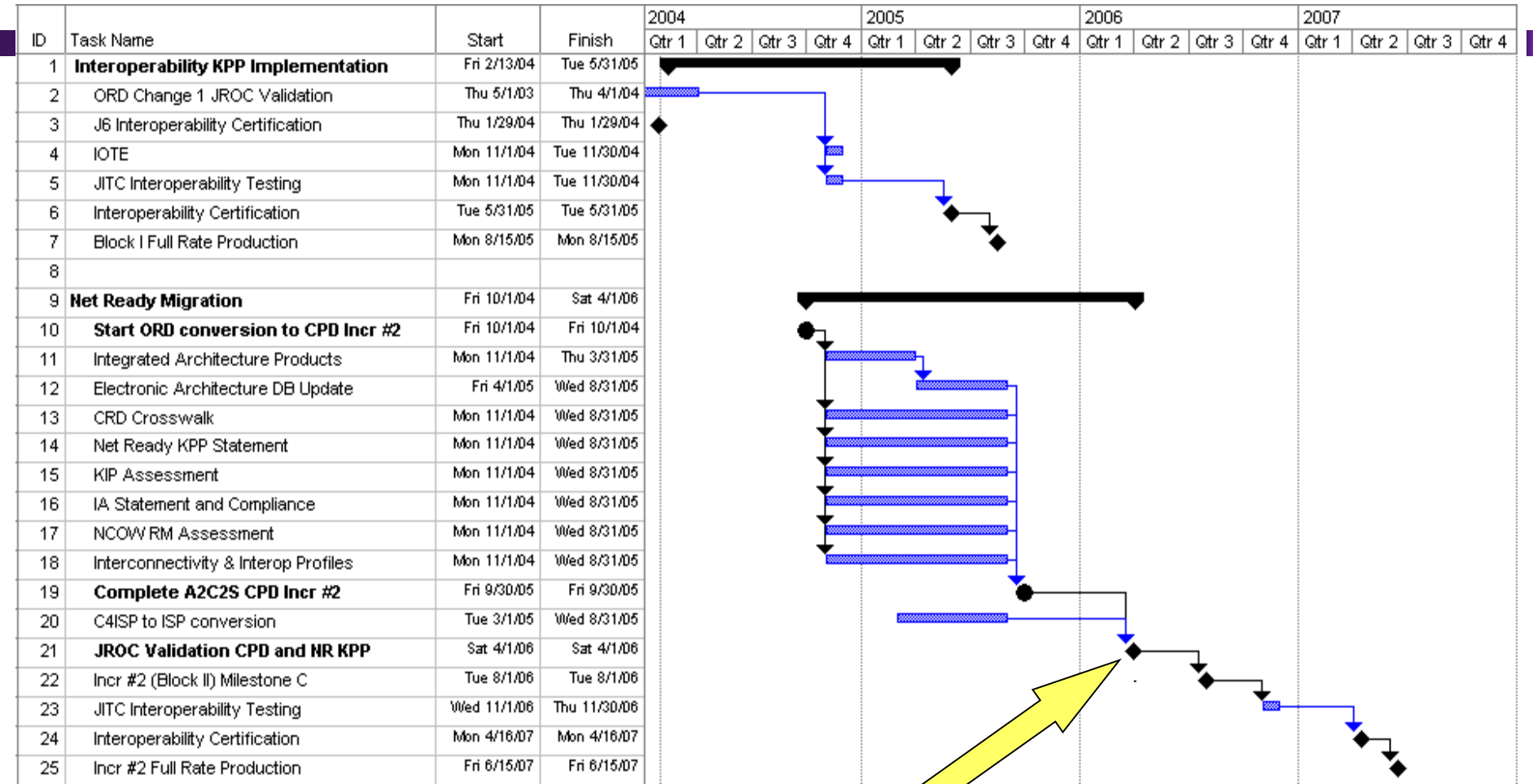


The following statement in the Interoperability Key Performance Parameter section of the document prior to proceeding to further review (re-staffing of the document is not required):

“The **<Document Sponsor>** will update the Interoperability Key Performance Parameter to include all applicable established components of the Net Ready Key Performance Parameter (NR-KPP) in accordance with CJCSI 62 12.0 1 C and a migration strategy to the remaining applicable components of the NR-KPP no later than **<date - no more than 6 months>.**”

This update will be submitted through the Joint Capabilities Integration and Development System (JCIDS) process for certification.

A2C2S Net Ready KPP Migration Plan



**Net Ready KPP Migration
Completed with JROC
Validation and Approval**



Example NR-KPP Transition/Certification Steps

CJCSI 6212.01C prescribes 7 steps for NR-KPP development/certification:

1. Develop the Mandatory Architecture Views
2. Complete CDD (ORD) CRD Crosswalk
3. Build a DISR online standards profile (TV-1)
4. Complete the initial LISI profile (Interface Requirement Profile) using the INSPECQTOR tool
5. Include the NR-KPP statement
6. Include the Key Interface Profile (KIP) Declaration
7. Include an IA statement of compliance

CJCSI 6212.01C provides criteria for J-6 Interoperability Requirements Certification (F-2) & Net Centric Assessment (F-3):

Sub Task 1:

Compliance with 24 certification criteria set in Table F-2

Sub Task 2:

Characterize FCS FoS net-centric attributes using the 24 Net Centric Assessment Criteria detailed in Table F-3



FCS Net Ready KPP Strategy

Team 1 Architecture

Mission Statement: **Develop mandatory NR KPP architecture views: AV1, OV2, 4, 5, 6C, SV4, 5, 6, and TV1**

End State: **Stake holder compiled and recommended series of views that reflect Operational concepts embodied by UA and demonstrate adherence to net readiness guidance**

Net-Ready KPP - Step 1

Product	Agency	Status	Remarks
AV-1	PM / LSI		AV1 to be delivered in LSI Produced <u>FCS Architecture Development Plan Overview and Summary All View -1</u> . CDRL A010 May 04.
OV-1	LSI / AIMD / UAMBL	 	High Level - From current ORD Version 2.0 of IPs 4, 5, 21, 23, and 24 (entire) selected for ORD inclusion.
OV-2	LSI / AIMD / UAMBL		
OV-3	LSI / AIMD / UAMBL		High Level from current ORD; OV3s for IPs resident in AARMS data
OV-4	LSI / AIMD / UAMBL		Aviation Squadron?
OV-5	LSI / AIMD / UAMBL		Will be part of next Architecture update (Sep 04)
OV-6c	LSI / AIMD / UAMBL		Currently Labeled Process Flow Diagram; Meets DODAF Description of OV6c
SV-1 / SoSV-1	LSI / PM		High Level - From current ORD Comanche, other complimentary systems, readability
SV-2	LSI		New Requirement
SV-4	LSI		Under Development. Jul 2004deliverable. CDRL A005
SV-5	LSI		Under Development. Jul 2004deliverable. CDRL A005
SV-6	LSI		Under Development. Jul 2004deliverable. CDRL A005
TV-1	PM / LSI / G6		TV 1 Requires Update to Conform to Evolving Guidance (JTA, ITA-A)



Team 1

Architecture

- **AV1 to be updated in LSI Produced FCS Architecture Development Plan Overview and Summary All View -1. (May 04, CDRL A010)**
- **OV5 Has Not Been Produced for this Version (2) of the Architecture. Version 3 of the Architecture will Include an OV 5 and will be Available by September 2004.**
- **All OVs Being Converted to UML**
- **Presentation of Data in Repositories**
- **SVs / TV1 (less SV1) to Support NRKPP are Under Development. CDRIL A005 delivery Jul 04.**

Architecture Development Timeline

	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV
AV1 (CDRL A010)								
SV2	New Requirement - Not Yet Contracted							
SV4 (CDRL A005)								
SV5 (CDRL A005)								
SV6 (CDRL A005)								
TV1 (CDRL A005)								



Team 2

CRD/ORD Crosswalk

Mission Statement: **Review / Update ORD to CRD Crosswalk**

End State: **Updated Appendix D to FCS ORD**

CRD-ORD Crosswalk



CRD	Class	Applicable	Status	Remarks
Advanced Military Satellite Communications (MILSATCM) CRD 24 Apr 1998		YES	☒	
Ballistic Missile Defense (BMD) JROC Draft 11 Oct 01		NO	☐	No specific applicability
Combat Identification (Combat ID) CRD 19 Mar 2001		YES	☒	
Close Air Support (CAS) CRD 6 May 2002		YES	☒	
Defense Information Systems Network (DISN) CRD 15 Apr 1996		NO	☐	Complying with higher level requirements of GIG
Distributed Common Ground / Surface Systems (DCGS) 6 Jan 2003		YES	☒	
Global Air Transportation Management (GATM) Phase I CRD 15 Nov 1999		NO	☐	Theater level transport aircraft
Global Air Transportation Management (GATM) Phase II CRD 2 Jun 2000		YES	☒	
Global Combat Support System (GCSS) CRD 27 Jun 2000		YES	☒	
Global Information Grid (GIG) CRD 30 Aug 2001		YES	☒	

CRD-ORD Crosswalk



CRD	Class	Applicable	Status	Remarks
Hard and Deeply Buried Target (HDBT) Defeat CRD 01 Dec 2000			●	
Imagery and Geospatial Information (I&GI) CRD 5 Oct 2000			●	
Information Dissemination Management (IDM) CRD 8 May 01		NO		Requirements incorporated in GIG CRD
Integrated Satellite Operations CRD Jan 2002		NO	○	No Space vehicles/control in UA
Space Control CRD 20 Mar 2000		NO	○	No Space vehicles/control in UA
Theater Air and Missile Defense (TAMD) CRD 01 Mar 2001		NO	○	
Theater Medical Information Program (TMIP) CRD 22 Feb 1999		YES	○	
Unified Cryptologic System CRD		YES	●	TS. Crosswalk not included here. Any crypto systems will be in compliance
United States Measurement And Signatures Intelligence CRD (USMS) 14 Nov 2002		YES	●	
Joint Deployment System (JDS) CRD March 2003		TBD	●	



Team 3

TV-1

Mission Statement: **Build a DISR online standards profile (TV-1)**

End State: **Initial TV-1 complete to facilitate ORD staffing NLT
12 MAR 2004**



Team 4

LSI Profile

Mission Statement: **Complete initial LSI profile using INSPEQTOR tool.**

End State: **Initial LSI profile complete to facilitate ORD staffing NLT 12 MAR 2004**

Team 4

LISI Profile



- **Step 4 - Complete the initial LISI profile (Interface Requirement Profile) using the INSPECQTOR tool. This profile is required prior to submitting the CDD. See Enclosure K.**
- **Enclosure K - Interconnectivity and Interoperability Capability (IIC) Profile.**
 - **IIC is composed of 2 elements**
 - **Interconnectivity Profile**
 - **Interoperability Capabilities Profile (generated through LISI questionnaire and report generator in Inspector)**



Team 5

NR KPP Statement

Mission Statement: **Finalize draft NR KPP statement and begin electronic staffing.**

End State: **Draft NR KPP sent to appropriate communities for staffing and comments received prior to 12 MAR 2004**

DRAFT FCS NR-KPP



Increment 1: FCS FoS activity interfaces, services, policy-enforcement controls, and data-sharing of the NCOW-RM and GIG-KIPs will be satisfied to the requirements of the specific Joint integrated architecture products (including data correctness, data availability and data processing), and information assurance accreditation.

Rationale: The FCS-equipped UA will operate as part of a Joint Team across DOTMLPF, supporting operations vertically and horizontally, from alert through deployment and employment. Given Joint Communications support and bandwidth between JTF, intervening HQ as established, and UA, [the FCS FoS will meet 100 percent of interfaces; services; policy-enforcement controls; and data correctness, availability and processing requirements designated as enterprise-level or critical in the Joint integrated architecture (Threshold) and 100 percent of interfaces; services; policy-enforcement controls; and data correctness, availability and processing requirements in the Joint integrated architecture (Objective)].



Team 5

NR KPP Statement Issues

- **IKPP placement vice NR KPP**
- **NR statement**

Team 6

KIP Declaration Issues

- **Developed Declaration**
- **FCS must comply with all 17 KIPs**
- **Awaiting approval of format**

Appendix J Network Ready KPP
TAB # (Key Interface Profile Declaration)

KEY INTERFACE PROFILE DECLARATION		
KIP	FCS Applicable	ORD Reference
KIP 1 Logical Network to DISN Transport Backbone	Yes	ORD 3156, ORD 3470, ORD 3447, ORD 3752 Base ORD paragraph 5.3.1, Annex H 2.5.2.11.2
KIP 2 Space to Terrestrial Interface	Yes	ORD 2401, ORD 3749
KIP 3 JTF to Coalition	Yes	ORD 1120, ORD 3752, ORD 2202
KIP 4 JTF Components to JTF HQ's	Yes	ORD 1120, ORD 3462 , Base ORD paragraph 1.5, Base ORD paragraph 1.5.1.2
KIP 5 STEP and TELEPORT	Yes	Annex H paragraph 2.5.2.11.2, ORD 2401
KIP 6 Joint Interconnection Service	Yes	ORD 3754, ORD 3752
KIP 7 DISN Service Delivery Point	Yes	Base ORD paragraph 5.3.1
KIP 8 Secure Enclave Service Point	Yes	ORD 2395, ORD 3749
KIP 9 Application to Database Server	Yes	ORD 2326, ORD 3249, ORD 3752 , Annex H paragraph 2.5.1.3.2
KIP 10 Client Server	Yes	ORD 2401 , Annex H paragraph 2.5.1.3.1.1.8
KIP 11 Application to COE/CCP	Yes	ORD 2401 , Annex H paragraph 2.5.1.3.1.1.8
KIP12 End System to PKI	Yes	Base ORD paragraph 5.3.1, Base ORD paragraph 5.3.4,
KIP 13 Management system to (Integrated) Management Systems	Yes	ORD 2326, ORD 3426
KIP 14 Management Systems to Managed Systems	Yes	ORD 3450
KIP 15 IDM to Distribution Infrastructure	Yes	ORD 2394, ORD 2413, ORD 3450
KIP 16 Information Servers to IDM Infrastructure	Yes	ORD 2392, ORD 2394, ORD 2413, ORD 3450
KIP 17 Applications to Shared Data	Yes	ORD 3158, ORD 3754, ORD 1064 , Annex A paragraph 1.3.1, Annex H paragraph 2.5.1.3.2, Annex H paragraph 2.5.1.3.1.9

The KIP definitions used came from www.kips.disa.mil



Team 7

IA Statement

Mission Statement: **Integrate IA compliance statement into ORD IAW appropriate DOD references.**

End State: **IA Compliance Statement complete to facilitate ORD staffing NLT 12 MAR 2004**

Team 7

IA Compliance



- **IA Team evaluation indicates we meet IA compliance**
- **Recommended statement of IA compliance:**
This system is currently in full compliance with DOD Directive 8500.1 and DOD Instruction 8500.2, and with Phase 1 Definition of the DITSCAP (DOD Instruction 5200.40), and has made the required Information Assurance documentation available to the Joint Staff J-6 for review.
- **DITSCAP**
 - **Phase 1 SSAA documents are in draft form (one for TS, one for Secret and below).**

Today- IER Based I KPP

FY04 - FY 06 NET READY KPP

Current Interoperability KPP (I KPP) Centers around one DOD Architectural Operational View (OV-3) that contains Information Exchange Requirements (IER)

Net Centric Operations Warfare
NCOW Reference Model Compliance

Integrated
Architecture

Information
Assurance

*Applicable
KIPs

Measurable and Testable Net-Ready KPP

FY06 NET READY KPP

- Net Centric Operations Warfare (NCOW) Reference Model Compliance
- Integrated Architecture
- Key Interface Profiles (KIPs)
- Information Assurance

FY06 and Beyond - NET READY

Net Ready approach centers on Central network:

- Focus on organizational contributions and consumption of information
- One-to-Network paradigm

Measurable and Testable Net-Ready KPP

Complementary and Corresponding Systems



- **GIG BE**
- **JTRS**
- **GCCS**
- **NCES**
- **TCS**
- **Crypto Modernization**
- **Collaboration Tools**
- **Horizontal Fusion**



Questions?



BACKUPS

Enforcement



- **If a program/system fails to meet certification requirements, the J-6 will not validate the program and will recommend the program not proceed to the next milestone and that funding be withheld until compliance is achieved and the program/system is validated. The J-6 will make this recommendation to the USD (AT&L), USD (P), USD (C), ASD (NII), the MCEB, and the JROC. The J-6 will also request that the program/system be added to the DOD 4630.8, Interoperability Watch List (IWL).**